الجمهورية الجزائرية الديمقراطية الشعبية
People's Democretic Republic of Algeria
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research

UNIVERSITÉ DE BISKRA

كلية العلوم والتكنولوجيا
قسم الهندسة الكهربائية

مذكرة ماستر

MASTER

العلوم والتكنولوجيا
شعبة: الاتصالات
تخصص: شبكات واتصالات

رقم: .....

إعداد الطالب(ة):
بوغزولة وسام&العلواني شهرزاد

يوم: 26 جوان 2022

التبادل الآمن للخادم والعميل

Secure client/server exchange

لجنة المناقشة:

أ. طبش سعاد	أ. تع أ	جامعة بسكرة	رئيسا
أ. قصباية الطاهر	أ. مح أ	جامعة بسكرة	مشرفا
أ. ذيابي فتحي	أ. مح ب	جامعة بسكرة	مناقشا

السنة الجامعية: 2021 – 2022

الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research

جامعة محمد خيضر بسكرة
كلية العلوم والتكنولوجيا
قسم الهندسة الكهربائية
شعبة: الإتصالات
التخصص: شبكات واتصالات

أطروحة التخرج

للحصول على درجة الماستر

التبادل الآمن للخادم/العميل

تقديم :
بوغزولة وسام
العلواني شهرزاد

الرأي الإيجابي للمشرف:
أ. قصباية الطاهر

رأي إيجابي لرئيس لجنة التحكيم
أ.طبش سعاد

ختم و توقيع

ملخص

في بيئة تكنولوجيا المعلومات الحديثة، وظائف مثل مواقع الويب، والتطبيقات المستندة إلى الويب، نظام الحوسبة المركزية، تطبيقات الهاتف المحمول او حتى الحوسبة السحابية، تعمل جنبا الى جنب مع مفهوم خادم العميل. تضع حوسبة العميل الخادم دورا حيويا في البيانات او المعلومات التي يتم تخزينها عن بعد و عمليات التبادل بين الغالبية. يلعب نظام خادم العميل دورا مهما في تطور تكنولوجيا المعلومات. المكونات المتضمنة في نظام العميل/الخادم مقسمة الى قسمين رئيسيين مكونين ماديين ومنطقيين. المكونات المادية هي الخوادم و أجهزة العميل و أجهز ة االدخال/اإلخراج و الشبكات و امدادات الطاقة اما المكونات المنطقية هي صفحات الويب و البيانات وبرامج البرمجة النصية والبروتوكو الت مثل IP، http، API، Telnet. في الجانب النظري من العمل تطرقنا الى نموذج خادم العميل كونه احد اهم النماذج التي تعتمد عليها الشبكات في ارسال البيانات بسبب سهولةً االرسال، وكون البيانات المتبادلة عن طريق المقابس قد تكون سرية او حساسة فهو في حاجة الى أنظمة حماية من السرقة و التغيير للكم الهائل من الخسائر التي ستقع في تفاديا كافة المستويات بعدم توفير القدر الكافي من الحماية، في الجانب التطبيقي قمنا بتصميم نموذج الخادم/العميل المؤمن بأحدث أساليب الحماية خوارزمية معيار التشفير المتقدمAES .

Abstact

In the modern information technology environment, functions such as websites, web-based applications, centralized computing system, mobile applications or even cloud computing, work hand in hand with the client-server concept. Server-client computing places a vital role in the data or information that is stored Remote and exchanges between the majority. The client-server system plays an important role in the evolution of information technology. The components included in a client/server system are divided into two main parts, physical and logical components. The physical components are servers, client devices, I/O devices, networks, and power supplies. The logical components are web pages, data, scripts, and protocols such as IP, http, API. Telnet. In the theoretical side of the work, we touched on the client-server model as it is one of the most important models on which networks depend in sending data because of the ease of transmission, and the fact that the data exchanged through sockets may be confidential or sensitive, it needs systems to protect against theft and change in order to avoid the huge amount of Losses that will occur at all levels by not providing enough protection, in the application we have designed a client/server model that is secured with the latest protection methods AES algorithm.

إهداء

الحمدلله الذي بنعمته قد وصلنا لهذا اليوم وهذا النجاح بفضله تعالى.

أهدي هذا العمل وهذا النجاح إلى من أنارت دربي وكانت سبب قوتي دائما، إلى من علمتني الصبر والإجتهاد، إلى أغلى جوهرة في حياتي، إلى بحر الحب من زينت حياتي *"أمي الغالية".*

إلى سندي وعزوتي، إلى أمان البيت، إلى من حصد الأشواك من دربي ليحميني ويعلمني"أبي الحبيب".

إلى أجزاء من روحي، القوة الخاصة بي، عكازي عند الضيق، الأثر الطيب في نفسي "حسام"، "إلياس"، "أمجد" إخوتي الأعزاء.

إلى زهرتي حياتي، بسمتي في الحياة، أملي في المستقبل، شمعتي عند الظلام "تسابيح الضحى"، "مرام" أختي الحبيبتين.

إلى من لم أرى في طيبتها وكرمها، من كانت تمنح دون أن تنتظر الرد، من شجعتني دائما وتمنت ودعت لي بالتوفيق الدائم، "جدتي العزيزة" ألبسك الله ثوب عافيته وشفاك وحفظك لنا.

إلى رفيقة طريقي ومشواري ومشروعي، الصادقة النية، أشكرك لوجودك رفيقة دربي الرائعة "بوغزولة وسام" صديقتي الغالية.

إلى الأستاذ المشرف المحترم "قصباية الطاهر" لإختياره هذا الموضوع القيم، وعلى النصيحة والتوجيه والإرشاد.

العلواني شهرزاد

إهداء

الحمد لله حمدا كثيرا اذ بلغني نجاحي هذا و الشكر له وحده لا شريك له

اهدي هذا العمل لارواح غالية انتقلت إلى جوار الله و هي في جواري لا تغيب و في قلبي حية لا تموت ذكراها أمي و أخي رحمهما الله و اسكنهما فسيح جناته.

اهديه للوالد الكريم حفظه الله وأدام عليا نوره و دعمه و سنده و أطال في عمره.

اهديه لأخواتي و أخي السند الدائم والظلع الثابت الداعمون لي عندما غاب الجميع.

اهديه إلى صديقاتي و رفيقاتي درب النجاح وادعو الله أن يحفظهم.

واهديه إلى شريكتي التي قاسمتني في مشروعنا هذا كل خطوة حتى النهاية.

بوغزولة وسام

شكر وتقدير

الحمد لله رب العالمين حمدا كثيرا طيبا مباركا فيه

الحمد لله وكفى والصلاة على الحبيب المصطفى وأهله ومن وفى أما بعد:

أولا الحمد لله والشكر له وحده لا شريك له على فضله إذ وفقنا لتثمين هذه الخطوة في مسيرتنا الدراسية بمذكرتنا هذه ثمرة الجهد والنجاح.

ثم الشكر كل الشكر للوالديين الكريمين على الدعم والتشجيع والتضحية من أجلنا ومن أجل بلوغ درجات عليا من النجاح بالغالي والنفيس ندعو الله أن يحفظهما.

الشكر والتقدير لكلا العائلتين من إخوة وأخوات الذين كانوا ومازالوا السند و الداعم الأول ، إلى رفيقات المشوار اللاتي قاسمننا لحظات النجاح رعاهم الله ووفقهم.

كما نتقدم بجزيل الشكر للمشرف السيد: قصباية الطاهر، الذي اقترح هذا الموضوع لنا وأدار العمل.

وإلى أعضاء لجنة التحكيم على اهتمامهم ببحثنا من خلال الموافقة على فحص عملنا وإثرائه بمقترحاتهم.

أخيرا، نشكر جميع الأشخاص الذين ساهموا بشكل مباشر أو غير مباشر في تحقيق هذا العمل.

القوائم

قائمة المحتويات

الفصل الثالث:التشفير والتأمين

الفصل الرابع: التطبيق

قائمة الأشكال

قائمة الجداول

المقدمة العامة

مقدمة عامة

منذ ظهور البشرية والتواصل ضرورة حيوية لا بد منها من أجل استمرارية الحياة، يتم هذا التواصل باستخدام الحواس كلها أو بعضها، أولاً بالصورة، ثم بالصوت، وأخيرا بالكتابة.

اليوم تربط الاتصالات السلكية واللاسلكية الناس البعيدة جغرافيا، وقد تم تطويرها وتحسينها بهدف البحث المستمر لإنتاج حلول أسرع، تعمل على نطاق كوكبي أو حتى مكاني.

تكون أجهزة الكمبيوتر مفيدة للغاية إذا كانت متصلة ببعضها البعض لمشاركة المعلومات والموارد، وتحتاج الشركات التي تضع أجهزة الكمبيوتر الخاصة بها على شبكة إلى اتخاذ بعض الاحتياطات البسيطة لتقليل مخاطر الوصول غير المصرح به.

الإنترنت عبارة عن شبكة عالمية تربط مليارات أجهزة الكمبيوتر التي تتواصل فيما بينها. سمح مدى هذه الشبكة بظهور العديد من الشركات التي تقدم خدمات متنوعة (الخدمات المصرفية عبر الإنترنت، البيع أو الشراء عبر الإنترنت، المراسلة، الشبكات الاجتماعية، إلخ).

تتطلب العديد من هذه الخدمات معلومات خاصة أو سرية قد يتضرر المستخدم في حالة سرقة أو فقدان هذه المعلومات. لهذا يتم دوما البحث عن طرق أمنية لحماية هذه المعلومات السرية.

تستعد العديد من الشركات الآن لليوم الذي سيتم فيه اختراقها بدلاً من توقع تكنولوجيا للحفاظ على سلامتهم وأمانهم طوال الوقت. غالبًا ما يتمكن المهاجمون من الدخول إلى شبكة شركة باستخدام أوراق اعتماد الموظفين المسروقة ولكن هذا فقط يمنحهم موطئ قدم، من هناك يحتاجون إلى استكشاف وتوسيع وجمع امتيازات الشبكة التي تساعدهم في الحصول على البيانات التي يريدون حقًا سرقتها، وكذلك الوصول إلى البيانات الشخصية للأشخاص العاديين بطرق مختلفة. نحن لا نهتم بكيفية وصولهم إلى هذا بقدر ما نشعر بالقلق إزاء حالة هذه البيانات من حيث الحماية، الطريقة الأكثر موثوقية لضمان سلامة أجهزة كمبيوتر الشركة هي الإمتناع عن وضعها على شبكة و إبقائها خلف أبواب مغلقة و للأسف هذا ليس حلا عمليا للغاية، و هنا تحتاج الشركات و الأفراد إلى تشفير البيانات بحيث إذا تمكن المتسللون من سرقة تلك البيانات، فلن يتمكنوا من فتحها أو استخدامها.

يعد نموذج الخادم / العميل والتشفير مجالات متجانسة توفر خدمات مفيدة تمكننا من استخدام الشبكات بأمان.

يهدف هذا المشروع إلى تصور وتنفيذ تطبيق فعال يستخدم التشفير كأداة لتشفير تبادل البيانات في نظام الخادم/العميل.

تتكون دراستنا من أربعة فصول:

في الفصل الأول، سنقدم نموذج الخادم / العميل بشكل عام، ثم سنناقش مكوناته، مزاياه وعيوبه مع ذكر هيكله وأنواعه.

أخيرًا، نتطرق الى احتياجات نموذج الخادم /العميل ونقدم مفهوم أولي للمقابس.

في الفصل الثاني، نعرض مقدمة عامة عن المقابس وأهميتها وفوائدها، كما سنقدم بعض التعريفات عن المقابس ومحيطها والتي تشمل أنواع المقابس وأنماط التوصيل وكيفية استخدام المنافذ للعناوين. نركز بشكل أساسي على الإجراءات الأولية التي تستخدم مآخذ التوصيل للتنفيذ.

في الفصل الثالث، نقدم مقدمة عامة عن التشفير، وطرقه الكلاسيكية والحديثة، وكيف يحفظ التشفير خصوصيتنا بمرور الوقت.

في الفصل الرابع، سنعرض المفهوم العام لتطبيقنا، ثم سنلقي نظرة على الوصف التفصيلي لكل نهج تم استخدامه، ثم سنقوم بتسجيل الدخول إلى قسم التنفيذ، والذي يتضمن الأدوات وبرمجة اللغة التي سنستخدمها، كما سنعرض تفاصيل التطبيق.

الفصل الأول
نموذج الخادم والعميل

1.1 مقدمة

مع استمرار أماكن العمل في استخدام البيانات المترابطة لأداء المهام اليومية، انتقل متخصصو تكنولوجيا المعلومات بشكل متزايد الى طريقة تعرف باسم نموذج الخادم/العميل لإدارة المعلومات.

تم استخدام مصطلح الخادم / العميل لأول مرة في عام 1980 للإشارة إلى أجهزة الكمبيوتر الشخصية على الشبكة وبدأ هذا النموذج يحظى بالقبول فعليا في أواخر الثمانينيات.

يستخدم مصطلح الخادم / العميل لوصف نموذج الكمبيوتر لتطوير الأنظمة المحوسبة، وبنيته بنية شبكة الكمبيوتر التي يطلب فيها العديد من العملاء (المعالجات عن بُعد) الخدمة ويتلقونها من خادم مركزي (كمبيوتر مضيف). غالبًا ما يتواجد العملاء في محطات العمل أو على أجهزة الكمبيوتر الشخصية، بينما توجد الخوادم في أماكن أخرى على الشبكة وتكون أجهزة أكثر قوة.

يستخدم هذا النموذج في توزيع الوظائف بين نوعين من الكيانات المستقلة: الخادم والعميل يكون نموذج الحوسبة هذا فعالاً بشكل خاص عندما يكون لكل من العملاء والخادم مهام مميزة يؤدونها بشكل روتيني. يمكن للعديد من العملاء الوصول إلى معلومات الخادم في وقت واحد وفي نفس الوقت، يمكن للكمبيوتر العميل أداء مهام أخرى.

في هذه الفصل، نقدم شرح لنموذج خادم العميل بشكل عام والأسئلة الشائعة المتعلقة بهذا الموضوع ونناقش خصائصه المختلفة، طوبولوجياه ومكونات العميل والخادم ثم نختم الفصل ببعض احتياجات نموذج الخادم/العميل.

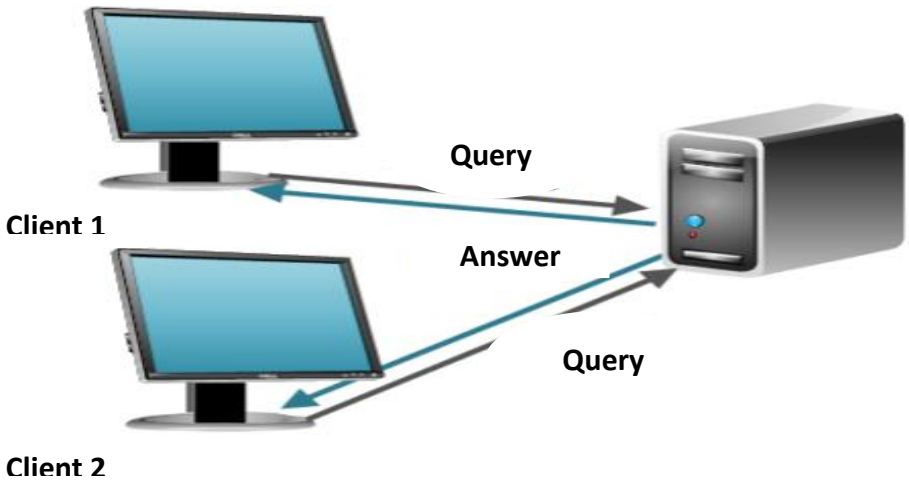
2.1 بنية الخادم/العميل

- **مفهوم نموذج الخادم/العميل**

نموذج خادم العميل هو اسم العملية المستخدمة لتوصيل المعلومات من الخادم إلى جهاز رقمي. يصف نموذج خادم العميل طريقة معينة للوصول إلى المعلومات المخزنة في الخوادم ليسمح للعديد من العملاء بفتح التطبيقات أو استرداد الملفات من خادم فردي، مما يساعد في الحفاظ على التناسق جميع الأجهزة.

يرسل العميل طلبًا إلى الخادم، ويعيد الخادم استجابة إلى العميل.

تُستخدم نماذج خادم العميل على نطاق واسع في جميع الصناعات التي تستخدم الخوادم لتخزين المعلومات والوصول إليها. [1]



الشكل 1.1: هندسة الخادم / العميل

- **الخادم**

عبارة عن مجموعة من البرنامج، يستمع إلى طلبات العميل التي يتم إرسالها عبر شبكة الاتصال. تقوم الخوادم بتنفيذ إجراءات مثل استعلامات قاعدة البيانات أو قراءة الملفات. تعمل عمليات الخادم عادةً على أجهزة الكمبيوتر المركزية المهيمنة أو محطات العمل. [2]

- **خصائص الخادم**

•هو مقدم الخدمة لذا يعمل على أجهزة كمبيوتر قوية وكبيرة (أجهزة قوية ونظام تشغيل قوي).

• يستمع وجاهز للرد على الطلبات المرسلة من قبل العملاء ولديه القدرة على التعامل مع أكثر من عميل في وقت واحد.

• بمجرد وصول الطلب إليه، يقوم بمعالجته وإرسال استجابة لمرسلها. [3]

- **العميل**

العملاء، المعروفون أيضًا باسم طالبي الخدمة، هم أجزاء من أجهزة الكمبيوتر أو برامج الخادم التي تطلب الموارد والخدمات التي يوفرها الخادم. [4]

تطبيق العميل هو عملية أو برنامج يرسل طلب وظيفة إلى خادم عبر شبكة الاتصال. تطلب هذه الوظائف من الخادم أداء مهمة معينة، مثل البحث عن سجل في قاعدة بيانات او غيرها من الطلبات. [2]

- **خصائص العملاء**

• هو مستهلك الخدمة فلا يتطلب أجهزة كمبيوتر قوية.

• يرسل طلبات إلى الخادم.

• ينتظر ويستقبل ردودًا من الخادم بعد انشاء الاتصال به. [3]

- **خصائص أنظمة الخادم/العميل**

العناصر التي تميز بنية الخادم / العميل هي:

• خدمة

نموذج الخادم / العميل هو علاقة بين العمليات التي تعمل على أجهزة منفصلة. الخادم هو مزود الخدمة والعميل مستهلك للخدمات.

• تقاسم الموارد

يعالج الخادم عملاء متعددين ويتحكم في وصولهم إلى الموارد.

• بروتوكول غير متماثل

نتيجة لمشاركة الموارد، يكون بروتوكول الاتصال غير متماثل حيث يبدأ العميل الحوار، ينتظر الخادم طلبات العميل.

• شفافية الموقع

يجب أن تخفي بنية الخادم / العميل موقع الخادم عن العميل (سواء كانت الخدمة على نفس الجهاز أو يمكن الوصول إليها عبر الشبكة). الشفافية عبر أنظمة التشغيل والأنظمة الأساسية للأجهزة.

• رسالة

الرسائل هي وسيلة الاتصال بين العميل والخادم.

• خدمات التغليف

الزبون يطلب الخدمة. يقرر الخادم كيفية جعله ترقية لبرنامج الخادم يجب ألا يكون لها أي تأثير على العميل طالما أن واجهة الرسالة هي نفسها.

• تطور

يجب أن تكون بنية الخادم والعميل قادرة على التطور أفقيًا (تطور عدد العملاء) وعموديًا (تطور عدد وخصائص الخوادم). [5]

3.1 تصنيفات الخادم والعميل

1.3.1 تصنيفات العميل

يتم تصنيف حوسبة العميل على أنها مكثفة، رقيقة أو مختلطة (هجين).

- **عميل مكثف Thick Client**: عميل يوفر وظائف غنية، ويقوم بمعالجة البيانات بنفسه، ويعتمد بشكل طفيف جدًا على الخادم.
- **العميل الرقيق Thin Client**: خادم العميل الرقيق عبارة عن كمبيوتر خفيف الوزن يعتمد بشكل كبير على موارد الكمبيوتر المضيف يقوم خادم التطبيق بمعظم الوظائف أي المعالجة المطلوبة للبيانات.
- **العميل الهجين Hybrid Client**: الذي يمتلك مجموعة من خصائص العميل الرقيق والعميل الكثيف، يعتمد العميل المختلط على الخادم لتخزين البيانات الدائمة، ولكنه قادر على المعالجة المحلية. [4]

2.3.1 تصنيفات الخادم

تتضمن بعض الأمثلة الشائعة للخوادم ما يلي:

- **خادم التطبيقاتApplication Server** : يستضيف تطبيقات الويب التي يمكن للمستخدمين في الشبكة استخدامها دون الحاجة إلى نسختهم الخاصة.
- **خادم الحوسبةComputing Server** : يشارك قدرًا هائلاً من موارد الكمبيوتر مع أجهزة الكمبيوتر المتصلة بالشبكة التي تتطلب قدرًا أكبر من طاقة وحدة المعالجة المركزية وذاكرة الوصول العشوائي أكثر مما هو متاح عادةً لأجهزة الكمبيوتر الشخصية.
- **خادم قاعدة البيانات Database Server**: يحافظ على قواعد البيانات ويشاركها لأي برنامج كمبيوتر يستوعب بيانات جيدة التنظيم، مثل برامج المحاسبة وجداول البيانات.
- **خادم الويبWeb Server** : يستضيف صفحات الويب ويسهل وجود شبكة

الويب العالمية حيث يسمح هذا النوع من الخوادم بتسهيل وصول العميل إلى الإنترنت. [4]

4.1 الطلب، الرد، وتوجيه تدفق البيانات

- **السؤالRequests**

رسالة مرسلة من قبل العميل إلى الخادم تصف العملية التي سيتم اجراؤها نيابة عن العميل.

- **الرد Responses**

تم ارسال رسالة بواسطة الخادم الى العميل بعد تنفيذ عملية تحتوي على معلمات الارجاع الخاصة بالعملية. [6]

يجب على العميل والخادم بالطبع استخدام نفس بروتوكول الاتصال. [7]

تنشأ مصطلحات العميل والخادم من أي جانب يبدأ الاتصال. بمجرد إنشاء الاتصال، يكون الاتصال ثنائي الاتجاه ممكنًا. في بعض الحالات، يرسل العميل سلسلة من الطلبات ويصدر الخادم سلسلة من الاستجابات. يمكن تلخيص المفهوم:

يمكن أن تتدفق المعلومات في أي من الاتجاهين أو كلاهما بين العميل والخادم. على الرغم من أن العديد من الخدمات ترتب للعميل لإرسال طلب واحد أو أكثر والخادم لإرجاع الردود[8].

5.1 نماذج الخادم/العميل

اعتمادا على طبيعة الخدمات التي يؤديها الخادم للعميل، تم تمييز أنواع مختلفة من الخادم/العميل:

1.5.1 الخادم/ العميل البيانات

في هذه الحالة، يضمن الخادم مهام الإدارة والتخزين ومعالجة البيانات.

هذه هي الحالة الأكثر شهرة للعميل / الخادم لاستخدامها من قبل جميع نظم إدارة قواعد البيانات الرئيسية. قاعدة البيانات مع جميع أدواتها (الصيانة، النسخ الاحتياطي ...) مثبتة على محطة عمل الخادم.

على العملاء، يتم تثبيت برنامج وصول يسمح بالوصول إلى قاعدة بيانات الخادم، يتم تنفيذ جميع عمليات معالجة البيانات على الخادم، والذي يقوم بإرجاع المعلومات التي يطلبها العميل. [5]

يجمع نموذج الخادم/العميل البيانات معًا البروتوكولات المخصصة لنقل البياناتSMB، FTP، NFS، POP إلخ. [7]

2.5.1 الخادم/العميل العرض التقديمي

في هذه الحالة، يتم الاستلاء على عرض الصفحات التي يعرضها العميل بشكل كامل بواسطة الخادم. هذه المنظمة لها مساوئ توليد حركة مرور كثيفة على الشبكة. [5]

يقوم نموذج الخادم / العميل العرض بتجميع البروتوكولات التي تهدف إلى السماح بجهاز التحكم عن بعد TELNET وSSH و11X وRDP وما إلى ذلك. [7]

3.5.1 الخادم/العميل المعالجة

في هذه الحالة، يقوم الخادم بإجراء المعالجة بناءً على طلب العميل، وقد يتضمن ذلك معالجة خاصة للبيانات، والتحقق من نموذج الإدخال، ومعالجة الإنذارات.

يمكن تحقيق هذه العمليات من خلال البرامج المثبتة على الخوادم ولكن أيضًا يتم دمجها في قواعد البيانات، وفي هذه الحالة، يتم دمج جزء البيانات وجزء المعالجة. [5] يقوم نموذج خادم / العميل المعالجة بتجميع البروتوكولات التي تهدف إلى التنفيذ عن بعد RPC، Java-RMI (JRMP)، CORBA-IIOP. [7]

6.1 طوبولوجيا الخادم / العميل

يشير مخطط الخادم / العميل إلى التخطيط المادي لشبكة هذا النموذج بتنسيق حيث يتم توصيل جميع العملاء والخوادم ببعضهم البعض. وهذا يشمل كل محطات العمل (العملاء) والخوادم.

التصميم الطوبولوجي للخادم / العميل المحتمل والاستراتيجيات المستخدمة هي كما يلي:

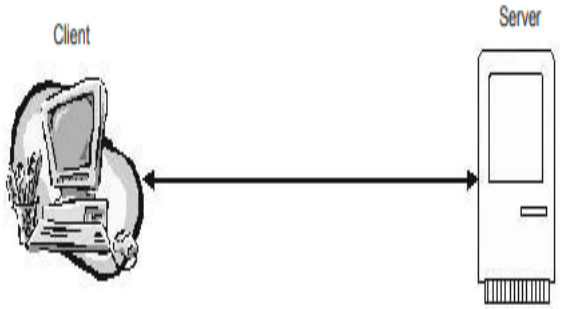
(1) عميل واحد، خادم واحد.

(2) عملاء متعددون، خادم واحد.

(3) عدة عملاء، خوادم متعددة. [9]

- **عميل واحد، خادم واحد**

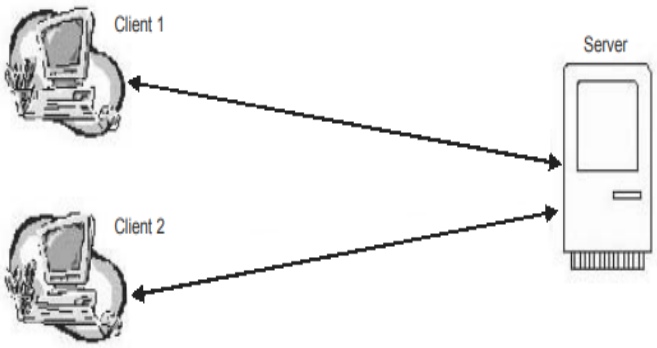
كما يوضح الشكل 1. 2، في هذا الهيكل عميل واحد متصل مباشرة بخادم واحد.



الشكل 2.1: عميل واحد، خادم واحد

- **عدة عملاء، خادم واحد**

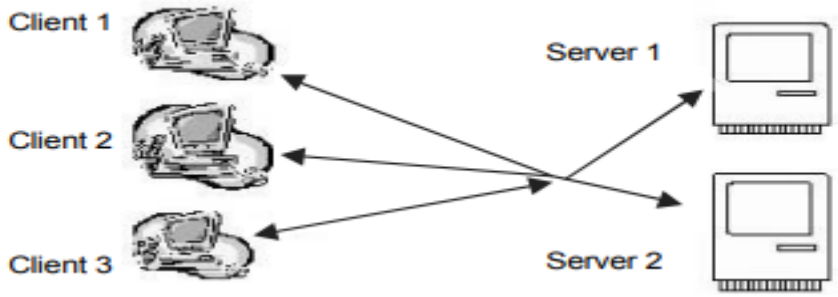
كما يوضح الشكل 3.1، في هذا الهيكل يرتبط العديد من العملاء مباشرة بخادم واحد فقط.



الشكل 3.1: عدة عملاء، خادم واحد

- **عدة عملاء، خوادم متعددة**

كما يوضح الشكل 4.1، في هذا الهيكل عدة عملاء مرتبطون بعدة خوادم.



الشكل 4.1: عملاء متعددون، خوادم متعددة

7.1 أنواع بنية الخادم/ العميل

تمثل الأنواع الأربعة من أطر عمل الخادم /العميل كيف تطورت العلاقة بين العميل والخادم مع تطورات الشبكات.

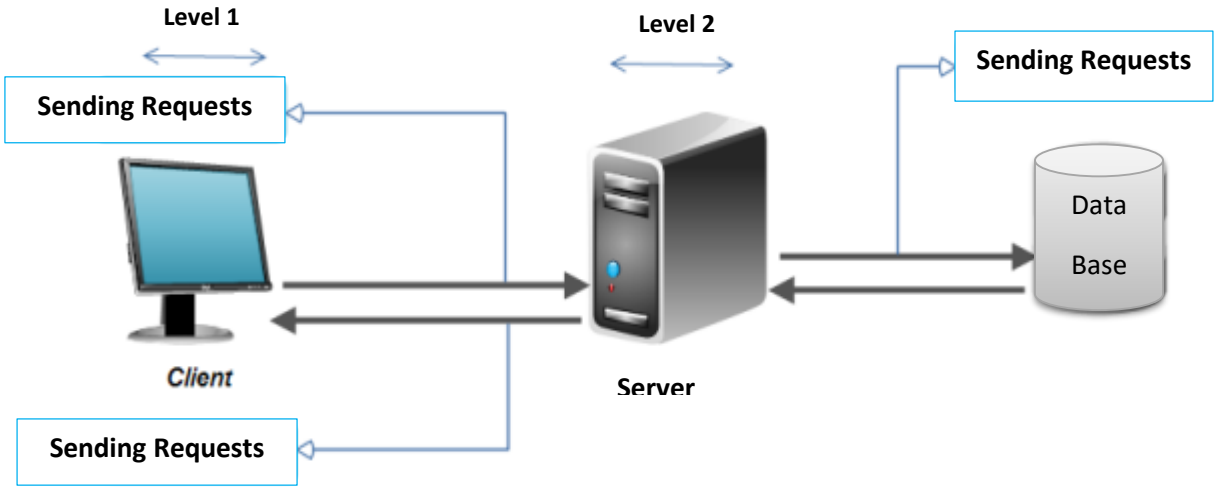
هناك أربع فئات رئيسية من حوسبة خادم العميل:

- **المستوى الأول: نظام الكل في واحد**

توجد جميع إعدادات تكوين خادم العميل وواجهة المستخدم ومنطق الأعمال ومنطق قاعدة البيانات على أجهزة الشبكة في بنية خادم العميل الأساسي. غالبًا ما تقتصر أطر العمل ذات المستوى الأول على الشبكات الأصغر حجمًا، وتشمل العرض التقديمي والأعمال وطبقات الوصول إلى البيانات على نفس الجهاز.

- **2-الطبقة: العميل والخادم**

تضيف معماريات المستويين خادمًا إلى المزيج وتفصل طبقة العرض التقديمي إلى واجهة مستخدم، حيث يقدم العميل طلبات خارج إمكانياته. يأخذ العملاء والخوادم المزيد من منطق الأعمال وقواعد البيانات على مستويات مختلفة، مما يوفر للمسؤولين بعض التحكم. [10]



الشكل 5.1: بنية الخادم / العميل ثنائية المستوى

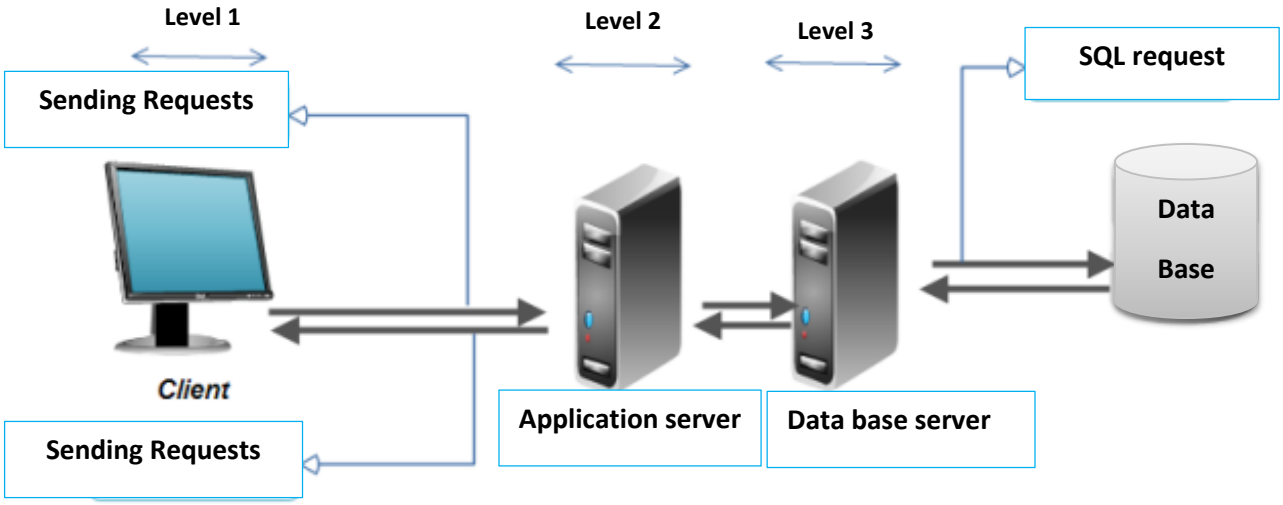
مزايا:

- الموارد المركزية: نظرًا لأن الخادم هو قلب البنية التحتية، يمكنه إدارة الموارد المشتركة لجميع العملاء، مثل قاعدة بيانات مركزية على سبيل المثال من أجل تجنب مشاكل التكرار و عدم الإتساق.
- أمان أفضل: حيث يوجد عدد أقل من نقاط الوصول إلى البيانات الأهمية.
- شبكة قابلة للتوسع: يمكن إزالة العملاء أو إضافتهم دون تعطيل تشغيل الشبكة وبدون إجراء تعديلات جوهرية.[11]

- **3-الطبقة: الوسيطة**

لمزيد من الحماية وإثراء البنية ثنائية المستوى، يشتمل هذا الإطار على برمجيات وسيطة بين طبقة العميل (طبقة العرض التقديمي) وطبقة الخادم (طبقة قاعدة البيانات).

توفر طبقة التطبيق هذه طبقة ثالثة، مما يتيح إدارة أكثر تعقيدًا لمنطق الأعمال. توفر أمثلة البرامج الوسيطة مثل خوادم تطبيقات الويب موازنة الحمل وزيادة التخزين والأمان.[10]



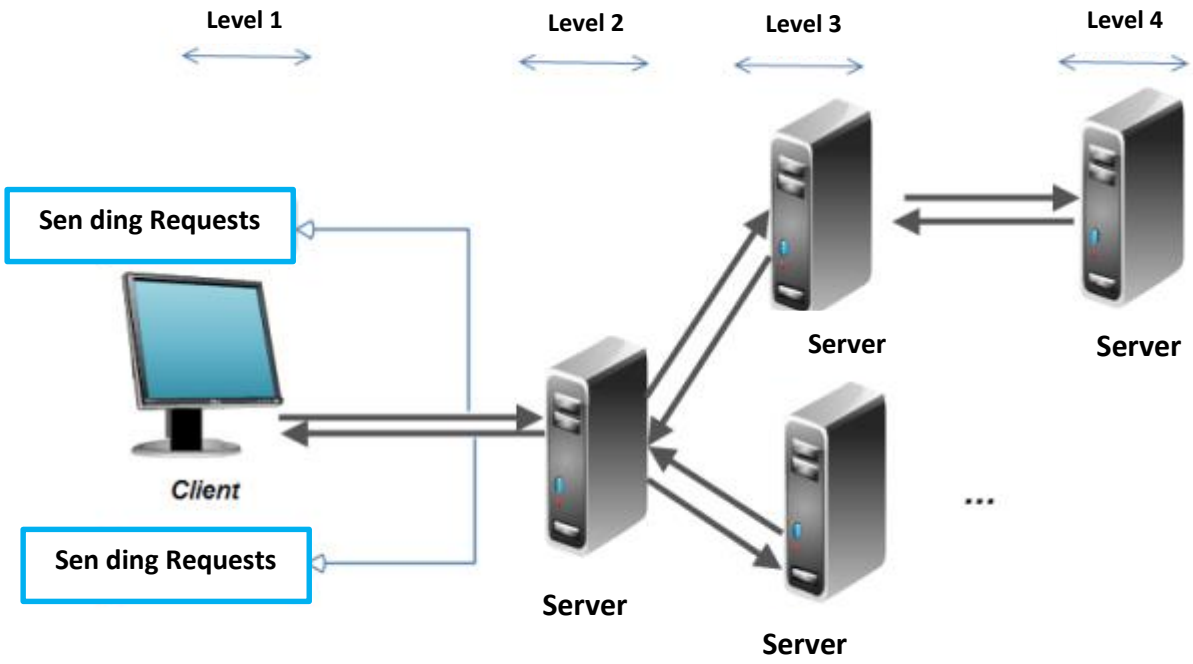
الشكل 6.1: بنية الخادم/العميل ثلاثية المستويات

بالإضافة إلى مزايا بنية العميل / الخادم، توفر هذه البنية الأساسية:

- الإدارة مركزية على مستوى الخادم لجميع العملاء الذين لديهم حق الوصول.
- أمان أكبر: يتم تحديده لكل خدمة.
- تمكين تكوين الأجهزة والبرامج غير المتجانسة لمحطات عمل العميل.
- الميل إلى الاقتران الضعيف: إمكانية استبدال مكون بآخر.
- توسيع نطاق إدارة المستخدمين المتزامنين. [11]

- **هندسة متعددة المستويات:N-Tiers**

يصف N-Tier، الذي يعمل خارج بنية 3-Tier، الاستخدام الإضافي للبرمجيات الوسيطة [3] ور
الشبكة ووظائفها. على الرغم من أن هذا يأتي مع قدر أكبر من التعقيد، إلا أن المؤسسات الحديثة تتطلب مرونة في البنى متعددة المستويات، وقابلية التوسع، والأمان. [10]



الشكل 7.1: بنية الخادم/العميل من المستوى N

المزايا

- تم تحسين الأداء العام.
- منطق الأعمال مركزي.
- تحقيق مستوى أمان محسن.

8.1 مزايا وعيوب شبكات خادم العميل

مزايا

- **مركزي:** النسخ الاحتياطي المركزي ممكن في شبكات خادم العميل، أي يتم تخزين جميع البيانات في الخادم.
- **الأمان:** هذه الشبكات أكثر أمانًا حيث يتم إدارة جميع الموارد المشتركة مركزيًا.
- **الأداء:** يزيد استخدام الخادم المخصص من سرعة مشاركة الموارد. هذا يزيد من أداء النظام العام.

- **قابلية التوسع:** يمكننا زيادة عدد العملاء والخوادم بشكل منفصل، أي أنه يمكن إضافة العنصر الجديد، أو يمكننا إضافة عقدة جديدة في الشبكة في أي وقت.

عيوب

- يعد الازدحام المروري مشكلة كبيرة في شبكات العميل / الخادم. عندما يرسل عدد كبير من العملاء طلبات إلى نفس الخادم قد يتسبب في مشكلة ازدحام حركة المرور.
- ليس لديها قوة الشبكة، أي عندما يكون الخادم معطلاً، فلا يمكن تلبية طلبات العميل.
- شبكة العميل / الخادم هي أمر حاسم للغاية. في بعض الأحيان، لا تخدم أجهزة الكمبيوتر العادية عددًا معينًا من العملاء. في مثل هذه الحالات، يلزم وجود أجهزة محددة في جانب الخادم لإكمال العمل.
- في بعض الأحيان توجد الموارد في الخادم ولكنها قد لا تكون موجودة في العميل. على سبيل المثال، إذا كان التطبيق على الويب، فلا يمكننا إخراج الطباعة مباشرة على الطابعات دون إخراج نافذة عرض الطباعة على الويب. [12]

9.1 مكونات نموذج خادم العميل

- **المكونات**

تعتمد بنية العميل/الخادم على مكونات الأجهزة والبرامج التي تتفاعل لتشكيل نظام.

يشتمل النظام بشكل أساسي على ثلاث مكونات:

. الأجهزة (العميل والخادم) .

. البرمجيات (التي تجعل الأجهزة جاهزة للعمل).

. البرمجيات الوسيطة للاتصالات.

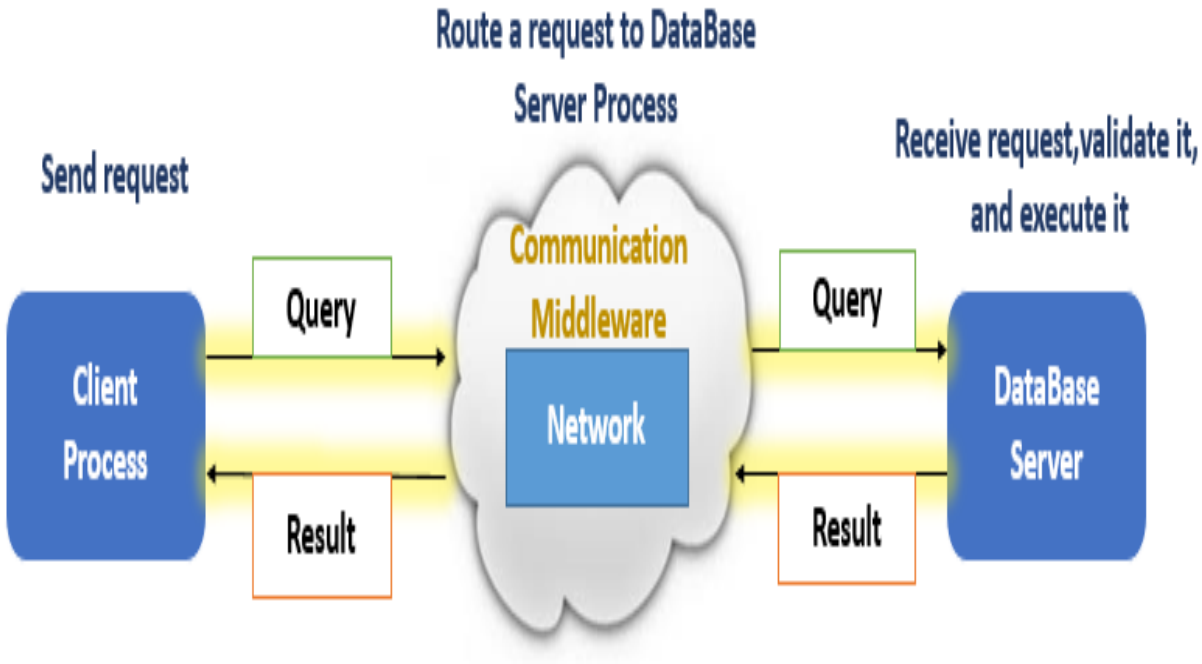
- **التفاعل بين المكونات**

ان آلية التفاعل بين مكونات بنية العميل/الخادم واضحة من الشكل حيث توفر عملية العميل الواجهة للمستخدمين النهائيين.

توفر البرمجيات الوسيطة للاتصالات كل الدعم الممكن للاتصال الذي يحدث بين عمليات العميل والخادم.

تضمن البرامج الوسيطة للاتصال ان الرسائل بين العملاء والخوادم يتم توجيهها وتسليمها بشكل صحيح.

يتم التعامل مع الطلبات بواسطة خادم قاعدة البيانات، الذي يتحقق من صحة الطلب و ينفذها و يرسل النتيجة مرة أخرى للعملاء. [9]



الشكل 8.1: تفاعل المكونات

- **امثلة عن مكونات الخادم/العميل**

الجدول التالي يعرض امثلة لكل من أجهزة الخادم، أجهزة العميل وأجهزة الشبكات. [10]

جهاز الشبكات امثلة	امثلة الخادم	امثلة العميل
Hub	خادم قاعدة البيانات	محطة العمل
Bridge	DNS	سطح المكتب
Switch	خادم تطبيق الويب	حاسوب محمول
Router	خادم الملفات	لوح
Gateway (بوابة)	Proxy Server	هاتف ذكي
Modem	Virtual Machine	IoT Device

جدول 1.1: امثلة عن مكونات الخادم/العميل

10.1 نموذج Open Systems Interconnection OSI

هو نظام في مجال شبكات الحاسوب المرجع الأساسي لترابط الأنظمة المفتوحة.

المرجع وضعته المنظمة الدولية للمعايير ISO سنة 1983 برقم 7498، ليكون نموذج نظري موثوق لبروتوكولات الاتصالات بين الشبكات الحاسوبية. وظائف الاتصال والتنظيم حسب مرجع ISO مقسمة على سبع طبقات مختلفة لكل طبقة دور يضم مجموعة مهمات يتطلب تحقيقها داخلها وعبر التواصل مع الطبقة التي تسبقها او التي تليها حسب الترتيب.

- **7.طبقة التطبيقات**

هذه الطبقة المسؤولة عن التطبيقات مثل البرامج التي يتعامل معها المستخدم مثل تصفح الانترنت يحتاج الى البرامج مثل برامج التصفح Chrome Google أو عندما يريد رفع ملفات إلى السيرفر أو سحب ملفات يحتاج ايضاً إلى برامج النقل مثل Client FTP أو عندما ا يحتاج لـ إرسال بريد أو استقبال بريد يحتاج برنامج Outlookكل هذه البرامج تعمل في طبقة التطبيقات.

البروتوكولات التي تعمل في طبقة التطبيقات SNMP، DNS، HTTP، DHCP، SSH،Telnet، SIP .

- **6. طبقة العرض**

هذه الطبقة المسؤولة عن تهيئة البيانات والتفريق ما بين كل نوع من البيانات وفي هذه الطبقة يتم العمل على اعداد واخذ كل امتداد على حسب نوع البيانات مثل النصوص والصور والفيديو والملفات المضغوطة وتقوم هذه الطبقة بعمل تشفير وفك التشفير للبيانات وتقوم بتغيير شكل البيانات إلى أشكال مختلفة إذا تطلب الامر وبعد أن تتم عملية التهيئة سيتم الارسال من جهاز المرسل إلى جهاز المستقبل والعكس.

البروتوكولات التي تعمل في طبقة العرض JPEG،MPEG، HTML .

- **5. طبقة جلسة العمل**

هي الطبقة المسؤولة عن ادارة وفتح واغلاق اية اتصال ما بين المستخدمين ومثال على ذلك عندما نقوم بفتح أكثر من موقع على شبكة الأنترنت نقوم بدخول على المتصفح ونقوم بدخول على أكثر من موقع في نفس الوقت ومن غير اية مشكلة هذا لان طبقة جلسة العمل تقوم بإدارة الاتصال وتنظيمه بينم.

البروتوكولات التي تعمل في الطبقة المسؤولة عن جلسة العمل RTP،SQL، NCP، SOCKETS .

- **4. طبقة النقل**

هذه الطبقة المسؤولة عن نقل وادارة البيانات وتحديد نوع البيانات المرسلة والمستقبلة وبعده تقوم بتحديد نوع البروتوكول المناسب للبيانات في عملية إرسال ونقل البيانات.

البروتوكولات التي تعمل في طبقة النقل UDP،TCP .

- **3. طبقة الشبكة**

هذه الطبقة المختصة في الشبكة هي المسؤولة عند ادارة الـ Packet تتم عملية التحويل إلى Packet بعد نزول الداتا من طبقة النقل layer Transport يتم نزول الداتا على شكل segment وبعد وصولها لطبقة الشبكة يتم تحويلها من segmentإلى Packet وبعده يتم إضافة IP جهاز المرسل وجهاز المستقبل وبعد هذه العملية تقوم هذه الطبقة بتحديد مسار الـ Packet الذي سيتم نقل البيانات منه والذي يسمى الموجه.

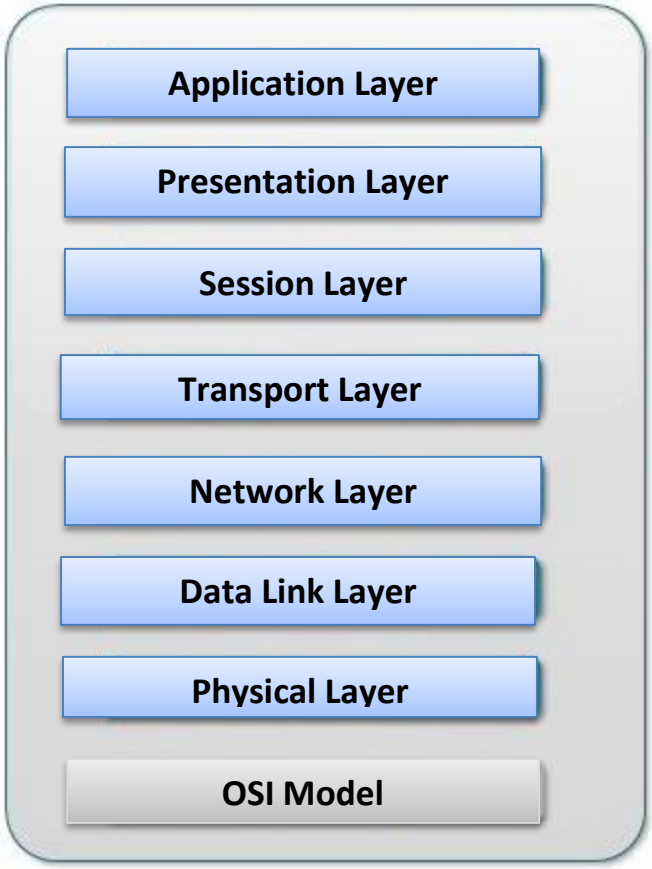
البروتوكولات التي تعمل في طبقة النقل OSPF،RIP

- **2. طبقة ارتباط البيانات**

طبقة ربط البيانات هي الطبقة التي يتم فيها تجهيز البيانات من أجل تسليمها للشبكة اي تحويل البت الخام إلى جدول من الاطارات. بشكل عام تكون مهمة طبقة ربط البيانات صنع خط فيزيائي يظهر الخطأ إلى الطبقات الأعلى وهذا ما يدعى بالدارة الافتراضية.

- **1.الطبقة المادية**

هذه الطبقة الأخيرة من الطبقات السبعة وهي آخر مرحلة تمر فيها البيانات أو الداتا بشكل نهائي ليتم ايصاله للجهاز المطلوب، وفي هذه المرحلة يتم تحويل الداتا أو البيانات عند الوصول لهذه الطبقة من شكلFrame إلى Bits 0 و1.



الشكل9.1: نموذج OSI

11.1 نموذج TCP / IP

لقد تم اختراعه سنة 1970، وكان جزء من أبحاث مؤسسة DARPA، التي قامت لتوصيل أنواع مختلفة من الشبكات وأجهزة الكمبيوتر. وكان تمويل هذه المؤسسة عاما من أجل تطوير هذه" اللغة"، ولذلك فإنها تتصف بعدم تبعيتها لاحد، والنتيجة أنها أصبحت ملكا عاما، وبالتالي لا يمكن لاحد ادعاء الحق باستخدامها له فقط . وأكثر من هذا فان بروتوكولات IP/TCP تتكون من عتاد Hardware وبرامج Softwareالبروتوكول بالنسبة للكمبيوتر على الانترنت عبارة عن مجموعة القواعد التي تحدد كيف يمكن لأجهزة الكمبيوتر أن تتفاهم مع بعضها البعض عبر الشبكة التي تتواجد عليها .وشبكة الكمبيوتر تعني جهازي كمبيوتر أو أكثر متصلة مع بعضها البعض وقادرة على أن تتشارك في المعلومات. عندما تتحدث أجهزة الكمبيوتر مع بعضها البعض فإن ذلك يعني تبادلها مجموعة من الرسائل. وحتى يكون في إمكانها فهم تلك الرسائل والعمل على تنفيذها فإن على أجهزة الكمبيوتر الموافقة على العمل بقواعد واحدة متفق عليها. [13]

- **1 . طبقة الشبكة المضيفة**

يتكون في الواقع من طبقتين: المادية والوصلة.

تصف الطبقة المادية الخصائص الفيزيائية للاتصال: الكابلات والموجات وما إلى ذلك.

تحدد طبقة الارتباط الوسيط المستخدم لتوجيه البيانات عبر الطبقة المادية: الكابل إيثرنت، واي فاي ...

- **2 . طبقة الانترنت**

يتمثل دورها في حقن الحزم في أي شبكة. عندما محطتين التواصل مع بعضها البعض عبر هذا البروتوكول، لم يتم إنشاء مسار لنقل البيانات في مقدمًا: يُقال إن البروتوكول "مستقل عن الاتصال". لذلك يمكن للحزم المرسلة الوصول خارج الترتيب لأنهم لن يتبعوا نفس الطريق. إنه بروتوكول النقل الذي سيكون مسؤولاً عن إعادة الطرود بالترتيب الصحيح.

- **3 . طبقة النقل**

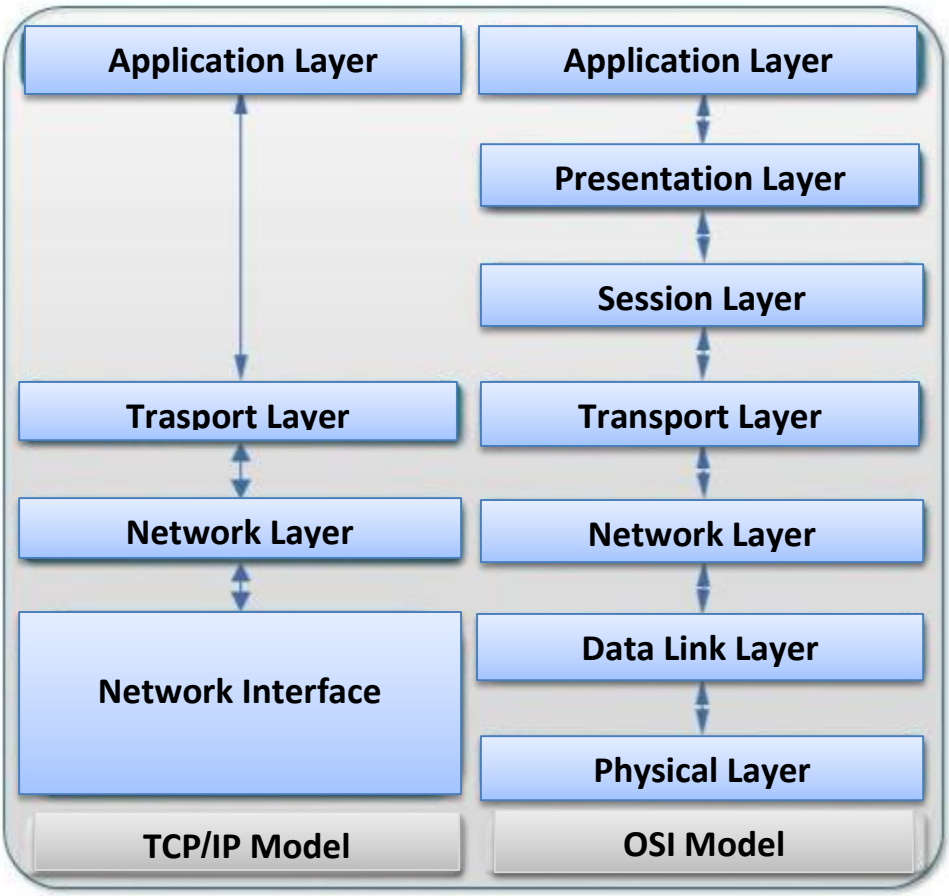
دورها مشابه لدور طبقة النقل لنموذج OSI. البروتوكولات المستخدمة لهذا الغرض المستوى هو TCP و UDP.

TCP عبارة عن حزم توجيه موثوقة وخالية من الأخطاء إلى الوجهة باستخدام الخدمات إقرار ، إدارة وقت الانتظار ، إلخ.

UDP غير موثوق به ولكنه أسرع. يتم استخدامه في الروابط الصوتية IP، حيث يفضل أن تفقد بعض البيانات ما يمكن توقعه. تستخدم أيضًا للدفق أو مؤتمرات الفيديو.

- **4. طبقة التطبيق**

يعتمد نموذج TCP / IP على ملاحظة أن برامج الشبكة تستخدم القليل جدًا، إن وجدت، طبقات الجلسة والعرض التقديمي. تتضمن هذه الطبقة جميع البروتوكولات عالية المستوى (FTP،SMTP، HTTP، DNS) سيتعين على هذه الطبقة اختيار بروتوكول نقل ملائم للخدمة. [14]



الشكل 10.1 نموذج TCP\IP

12.1 الوسيطة

- **مفهوم**

نسمي البرمجيات الوسيطة (أو برنامج الوسيط باللغة الفرنسية)، حرفيًا "عنصر الوسط"،

مجموعة طبقات الشبكة وخدمات البرمجيات التي تسمح بالحوار بين المكونات المختلفة للتطبيق الموزع. يعتمد هذا الحوار على بروتوكول تطبيق مشترك، محدد بواسطة واجهة برمجة التطبيقات الوسيطة.

الوسيطة هي واجهة اتصال عالمية بين العمليات. انه يمثل حقًا حجر الأساس لأي تطبيق عميل / خادم هذا هو البرنامج الذي يضمن إجراء حوارات بين العملاء والخوادم غير المتجانسين، أو بين

تطبيقين لا يحتويان على نفس واجهة برمجة التطبيقات. مصنوعة من "تكييف البروتوكول" للطبقات 5 و6 و7من نموذج OSI.

الهدف الرئيسي للبرمجيات الوسيطة هو توحيد الوصول والتلاعب لجميع الخدمات المتاحة على الشبكة، للتطبيقات، من أجل الاستفادة منها وجعل استخدامها شبه شفاف.

الشكل 11.1 البرامج الوسيطة

- **خدمات البرمجيات الوسيطة**

الوسيط قادر على تقديم الخدمات التالية:

التحويل: الخدمات المستخدمة للاتصال بين الأجهزة التي تطبق تنسيقات بيانات مختلفة.

عنونة: يسمح لك بتحديد جهاز الخادم الذي توجد عليه الخدمة المطلوبة من أجل استنتاج مسار الوصولبقدر الإمكان.

الأمان: يسمح لك بضمان سرية وأمن البيانات باستخدام آليات المصادقة على المعلومات وتشفيرها.

الاتصالات: يسمح بنقل الرسائل بين النظامين دون تغيير. يجب أن تدير هذه الخدمة الاتصال بالخادم، والإعداد لتنفيذ الطلبات، استرجاع النتائج وقطع الاتصال عن الاستخدام.

تخفي البرمجيات الوسيطة تعقيد التبادلات بين التطبيقات وبالتالي تجعل من الممكن رفع

مستوى واجهات برمجة التطبيقات التي تستخدمها البرامج. بدون هذه الآلية، ستكون برمجة تطبيق العميل/الخادم معقدة ويصعب قياسها. [5]

13.1 المقابس

لبرمجة تطبيق خادم العميل، من الملائم استخدام المقابس.

توفر المقابس واجهة تسهل استخدام بروتوكولات النقل مثل TCPو UDP

المقبس ببساطة هو وسيلة لتعيين نهاية قناة اتصال ثنائية الاتجاه على جانب العميل أو الخادم من خلال ربطه بمنفذ.

بمجرد انشاء قناة الاتصال بين عمليات العميل والخادم يمكن التواصل باستخدام نفس العناصر الأولية المستخدمة في الوصول إلى الملفات. [15]

14.1 الخاتمة

نموذج الخادم /العميل هو أساس جميع خدمات شبكات الكمبيوتر، وهذا سبب اهتمامنا بدراسة هذا النموذج. الغرض من هذا الفصل هو وصف المفاهيم الأساسية المختلفة لهذا النموذج الذي يعتبر أداة لتسهيل الاتصال وقدمنا شرح مفصل لأنواعه ونماذجه.

اختتمنا الفصل بتعريف مبدئي عن المقابس والتي ستكون موضوع فصلنا الثاني مع استعراض التعريف الشامل للمآخذ.

الفصل الثاني
المقابس

1.2 مقدمة

تتواصل عمليتان تعملان على نفس الجهاز أو أجهزة مختلفة من خلال المقابس، ويُنظر إلى المقابس على أنّها نهاية الاتصال ثنائي الاتجاه بين عمليتين، وتستخدم بشكل شائع في تطبيقات خادم/ العميل التي تسمح بالاتصال بين تطبيقات متعددة.

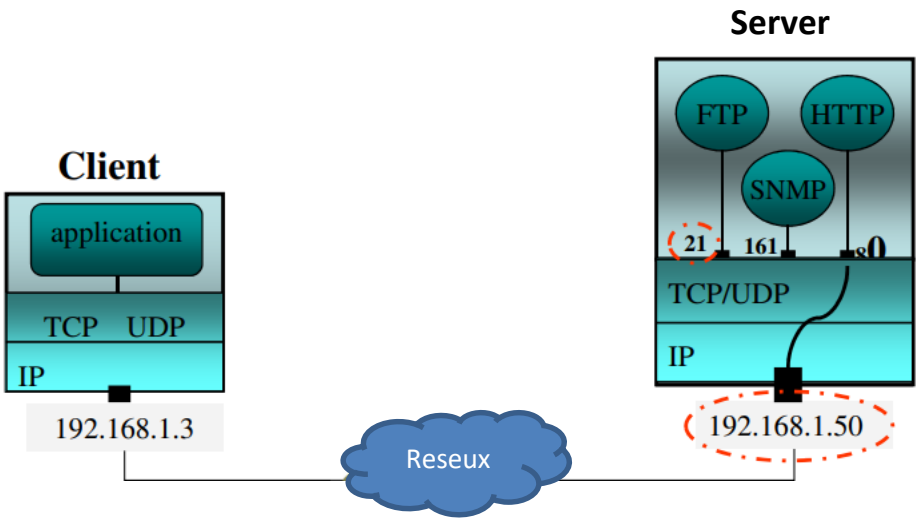
في هذا الفصل، نلقي نظرة معمقة على مرفق برمجة المقابس، بما في ذلك برمجة UDP وTCP القياسية للعميل / الخادم.

2.2 تعريف المقبس sockets

المعروف عالميا أيضا باسم مآخذ وهو عبارة عن فكرة مجردة يمكن للتطبيق من خلالها إرسال البيانات واستلامها وتوفير وصول عام إلى خدمات الاتصال بين العمليات مثلTCP/IP.[16]

وهي متوفرة الآن في جميع أنظمة يونكس الشائعة، المقبس هو مصطلح كمبيوتر يمكن أن يكون له عدة معانٍ اعتمادًا على ما إذا كان يُستخدم في البرامج أو الأجهزة. تسمح المقابس بالاتصال بين عمليتين مختلفتين على نفس الجهاز أو على أجهزة مختلفة. لكي نكون أكثر دقة، إنها طريقة للتحدث مع أجهزة الكمبيوتر الأخرى.

يسمح النموذج بالاتصال بين العمليات (IPC – الاتصال بين العمليات) من أجل السماح للعمليات المختلفة بالاتصال على نفس الجهاز وعبر شبكة TCP / IP.[25]



الشكل 1.2:عملية التواصل عبر مقبس

3.2 تاريخ

ظهرت المآخذ في عام 1983.مرفق برمجة توزيع برامج Berkeley Software Distribution (BSD) عبارة عن مجموعة من وظائف لغة البرمجة وأنواع البيانات، والتي تُعرف بواجهة برمجة تطبيق مآخذ BSD (API).

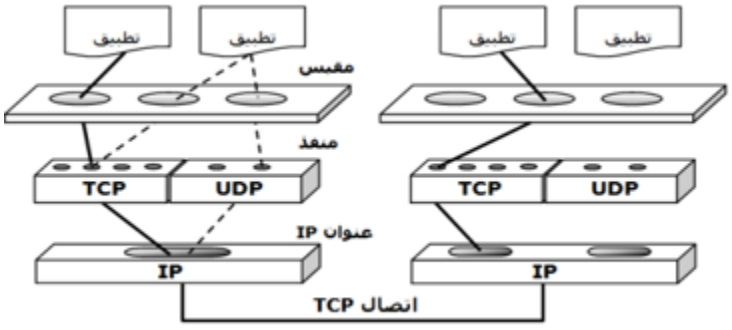
تم تقديم هذا المرفق لأول مرة مع نظام التشغيل BSD UNIX في أوائل الثمانينيات، ولكنه متاح الآن على معظم أنظمة التشغيل المشابهة لـ UNIX ومدعوم على نظام Microsoft Windows الأساسي.[24]

4.2 سبب اللجوء للمقابس

من أجل تمكين التطبيقات من أن تتصل بشبكة حاسوب وتتبادل البيانات مع غيرها من التطبيقات عبر الشبكة نفسها، تم إنشاء مفهوم المقبس socket، كتجريد، يشبه مفهوم واصف الملف filedescriptor، في سياق أنظمة التشغيل.

تتحكم البروتوكولات في عمليات الاتصال، لأنها هي التي تملي القواعد التي يجب أن يسير عليها جميع أطراف الاتصال. على الإنترنت، مجموعة بروتوكولات TCP/IP هي المسؤولة عن هذا الدور، المشكلة هنا أن حاسوباً واحداً ببطاقة شبكة وحيدة وعنوان وحيد قد يحتاج إلى أكثر من اتصال في نفس الوقت، وهنا لم يعد العنوان الواحد كافياً لتوصيل الرسائل إلى وجهتها. المثال على ذلك حاسوب خادم يوفر خدمة ويب، خدمة بريد وخدمة نقل ملفات فمن الواضح أن أكثر من نوع من الرسائل يصل إلى هذا الحاسوب، بعضها موجّه إلى برنامج خادم الويب، وبعضها يتصل ببرنامج خادم البريد، وآخر يتبادل الملفات مع برنامج نقل الملفات. كل الرسائل ستصل إلى نفس الجهاز (لأن له عنواناً واحداً)، لكن هذا غير كافٍ لإتمام الاتصال وتبادل البيانات بشكل صحيح ودون خلط. هنا يأتي دور بروتوكولات أخرى (من نفس مجموعة بروتوكولات TCP/IP)، في طبقة أخرى (طبقة النقل). هذه البروتوكولات (في الغالب الأعم إما TCP أو UDP)، هي المسؤولة عن إنشاء الاتصال ليس بين طرفين فحسب، وإنما بين تطبيقين محددين على كل طرف. هي مسؤولة عن تمييز الرسائل الواردة (والصادرة)، وإعطاء كل ذي حق حقه. من ذلك نعرف أن التطبيقات إن أرادت أن تتواصل فيما بينها، فلا بد لها من تحديد عنوان الطرف الآخر، وعنوان التطبيق النظير على ذلك الطرف، كمثال على ذلك منفذ 80 لخدمة الويب HTTP، ومنفذ 25 لخدمة البريد SMTP، ومنفذ 20 لخدمة نقل الملفاتFTP .[26]

باختصار: مجموع المكونات الثلاثة: عنوان IP ورقم منفذ وبروتوكول محدد هو اصطلاحاً مقبس.



الشكل 2.2: المقابس وعلاقتها بالعناوين والمنافذ

5.2 مبدأ عمل المقبس

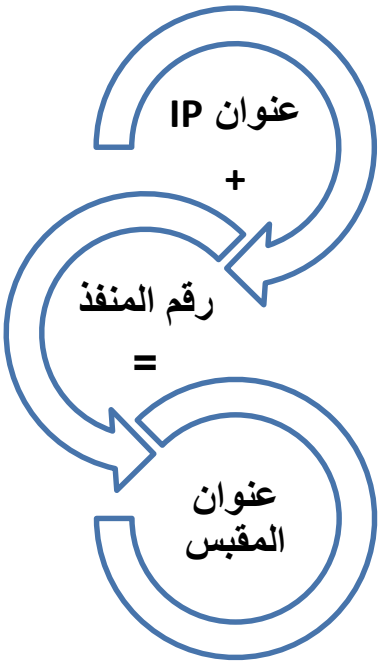
تستخدم المآخذ بشكل شائع للتفاعل بين العميل والخادم. يضع تكوين النظام النموذجي الخادم على جهاز واحد والعملاء على أجهزة أخرى. يقوم العملاء بالاتصال بالخادم، وتبادل المعلومات، ثم قطع الاتصال.

المقبس لديه تدفق نموذجي للأحداث. في نموذج العميل إلى الخادم المهيأ للاتصال، ينتظر المقبس الموجود في عملية الخادم الطلبات من العميل. للقيام بذلك، ينشئ الخادم أولاً (يربط) عنوانًا يمكن للعملاء استخدامه للعثور على الخادم. عند إنشاء العنوان، ينتظر الخادم العملاء لطلب الخدمة. يتم تبادل البيانات من العميل إلى الخادم عندما يتصل العميل بالخادم من خلال مقبس. ينفذ الخادم طلب العميل ويرسل الرد مرة أخرى إلى العميل. [21]

6.2 كيفية تحديد المقبس

يتم تحديد المقبس بواسطة العناصر التالية:

- عنوان IP أحد عناوين الجهاز.
- منفذ يتم تعيينه تلقائيًا أو اختياره بواسطة البرنامج.[19]



الشكل 3.2: انشاء عنوان مقبس

يتصل المقبس بمقبس آخر عبر عنوانه، أي اتصال ينطوي على مأخذين يجب أن يكون لهما نفس الخصائص:

- استخدام نفس البروتوكول.
- لها نفس نوع الاتصال. [18]

7.2 أنواع المقابس

تتوفر المقابس الأكثر استخدامًا في أربعة أنواع هي الدفق ومخطط البيانات بينما نادرًا ما تستخدم الخام وتسلسل الحزمة. تُستخدم العمليات المفترضة للتفاعل بين نفس النوع من المقابس مع عدم وجود قيود أخرى تمنع اتصال أنواع مختلفة من المقابس.

- **مقبس الحزمة المتسلسل** يوفر هذا النوع من المقابس اتصالاً موثوقًا به لمخططات البيانات التي يكون الحد الأقصى لطولها ثابتًا. هذا الاتصال ثنائي الاتجاه ومتسلسل.
- **مقبس مخطط البيانات** يتم دعم تدفق الرسائل ثنائي الاتجاه بواسطة مقبس مخطط البيانات. قد يتلقى جهاز الاستقبال في مقبس مخطط البيانات رسائل بترتيب مختلف عن ذلك الذي تم إرسالها به.
- **مقبس الدفق** تعمل مآخذ الدفق مثل محادثة هاتفية وتوفر تدفقًا موثوقًا به ثنائي الاتجاه للبيانات بدون حدود للتسجيل. تدفق البيانات هذا أيضًا متسلسل وغير مكرر.
- **مقبس خام** يستخدم هذا النوع لارسال حزمة معدلة داخل الشبكة ،عندما نريد انشاء بروتوكول لا يحتوي على معلومات الراس ستحتاج الى التعامل مع المقبس الخام. [19]

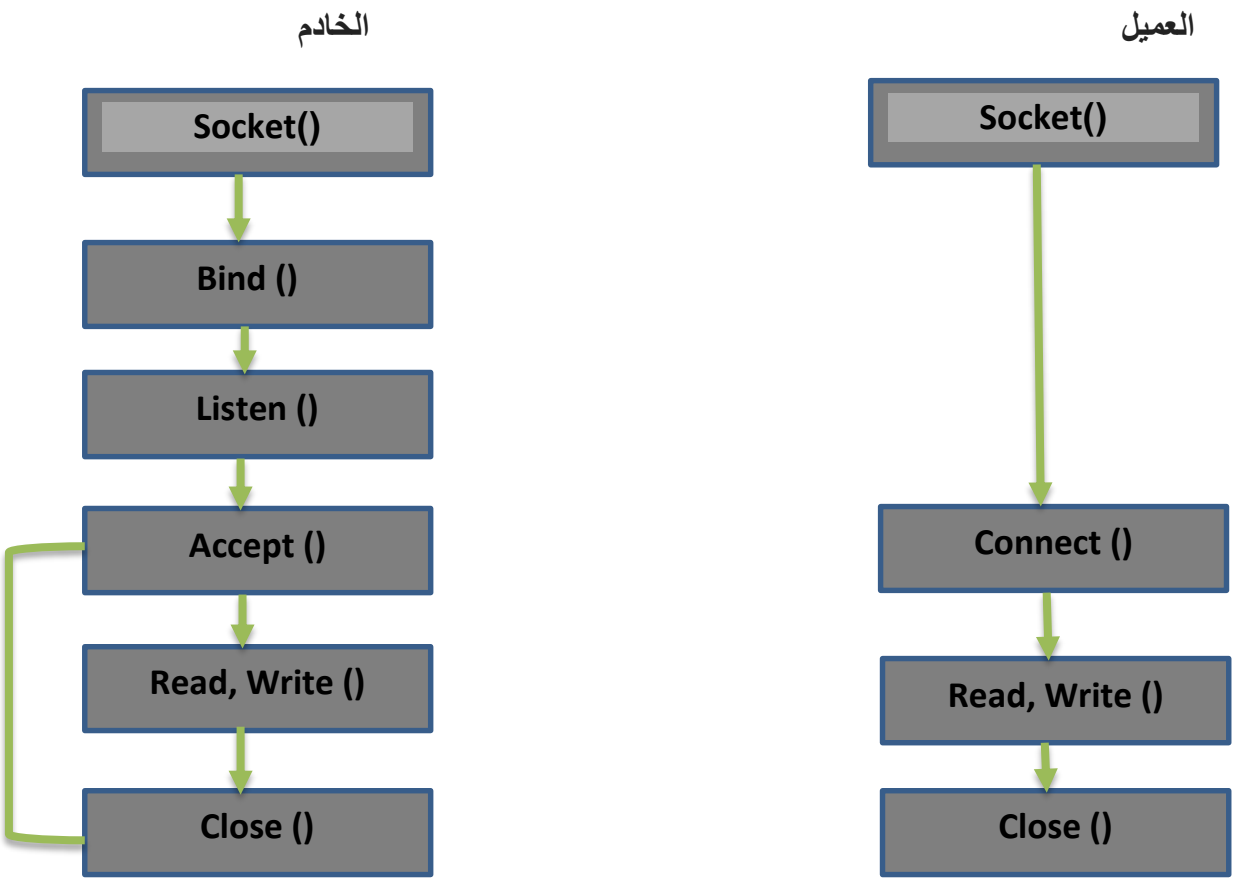
8.2 مآخذ الإجراءات الأولية

المعنى	مآخذ الإجراءات الأولية
قم بإنشاء نقطة نهاية اتصال جديدة	socket()
إرفاق عنوان محلي بمقبس	bind()
أعلن عن استعداده لقبول الاتصالات	listen()
حظر المتصل حتى وصول طلب الاتصال	accept()
حاول بنشاط إنشاء اتصال	connect()
أرسل بعض البيانات عبر الاتصال	send()
تلقي بعض البيانات عبر الاتصال	recv()
حرر الاتصال	close()

جدول1.2: مآخذ الإجراءات الأولية

لتسهيل استخدامها، تم تصميم مآخذ التوصيل للاحتفاظ بدلالات العناصر الأولية لنظام الإدخال / الإخراج تمامًا مثل الملفات (إنشاء، فتح، قراءة، كتابة، إغلاق). لتوصيل البيانات بين مأخذين، في وضع متصل، يجب التمييز بين الذي يستخدمه البرنامج الذي يطلب الاتصال (العميل) والآخر المستخدم من قبل البرنامج الذي يقبل الاتصالات (الخادم). الخادم هو برنامج ينتظر الاتصالات من خلال مقبس ثم يعالج جميع الاتصالات الواردة.العميل هو برنامج يتصل بخادم من خلال مقبس.

يوضح الرسم البياني التالي الخطوات المختلفة التي يقوم بها العميل والخادم للتواصل. [17]



الشكل4.2: خطوات التواصل بين الخادم والعميل

9.2 مقبس API

تعني واجهة برمجة التطبيقات، وهو حل برمجي يسمح لتطبيقين بالتواصل مع بعضهما البعض. في كل مرة تستخدم فيها تطبيقًا مثل Facebook، أو ترسل رسالة فورية، أو تتحقق من الطقس على هاتفك، فأنت تستخدم واجهة برمجة تطبيقات.

لا ترى تطبيقات العميل /الخادم الا طبقات الاتصال من خلال واجهة برمجة تطبيقات.

يجب على العملية التي ترغب في الاتصال بعملية أخرى انشاء مثيل مثل هذا البناء، تصدر العمليتان العمليات التي توفرها واجهة برمجة التطبيقات لإرسال واستلام البيانات. [5]

- **وظائف مقبس واجهة برمجة التطبيق socket API**

Socket API عبارة عن مجموعة من استدعاءات مأخذ التوصيل التي تمكنك من أداء وظائف الاتصال الأساسية التالية بين برامج التطبيق:

*القيام بإعداد وإنشاء اتصالات للمستخدمين الآخرين على الشبكة.

*إرسال واستقبال البيانات من وإلى المستخدمين الآخرين.

*إغلاق الاتصالات.[22]

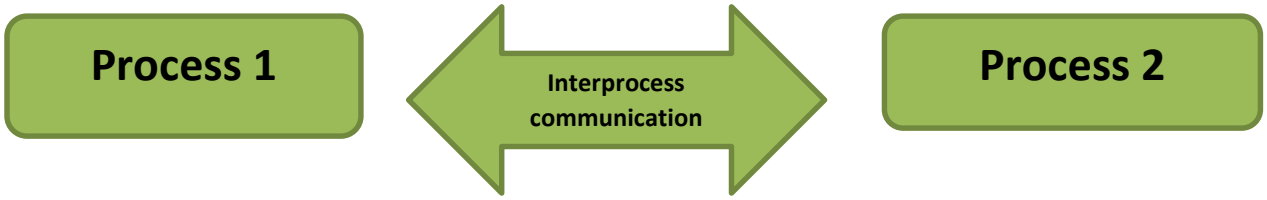
10.2 الاتصال بين العمليات interprocess communication IPC

يسمح المقبس بالاتصال بين العمليات التي تعمل إما على نفس الجهاز أو على أجهزة مختلفة. تم استخدامه عالميًا (UNIX ، Linux، Windowsوما إلى ذلك)[18]. الاتصال بين العمليات هو العمود الفقري للحوسبة الموزعة. في الحوسبة، يعد الاتصال بين العمليات (IPC) مجموعة من الآليات التي تسمح للعمليات المتزامنة بالاتصال. يمكن تصنيف هذه الآليات إلى ثلاث فئات:

–الآليات التي تسمح بتبادل البيانات بين العمليات.

–الآليات التي تسمح بالمزامنة بين العمليات (على وجه الخصوص لإدارة مبدأ القسم الحرج).

–الآليات التي تسمح بتبادل البيانات والتزامن بين العمليات. [23]



الشكل 5.2: الاتصال بين العمليات

11.2 أنواع خدمة النقل عبر المقبس API

نميز نوعان من خدمة النقل عبر المقبس API وهما

- مقبس الدفق مع بروتوكول مهيأ للاتصال TCP
- بروتوكول مخطط بيانات المستخدم UDP

يوجد أساسًا بروتوكولا اتصال لكل مقبس، أحدهما عن طريق TCP والآخر بواسطة UDP. عموماTCP موثوق لأنه يتطلب نقطة التقاء بين العميل والخادم في وقت اتصال العميل يتم التأكد من وجود الطرفين في وقت الاتصال. من ناحية أخرى في UDP، لا توجد نقطة عودة، وبالتالي فإن الخادم ليس متأكدًا من تلقي المعلومات بالفعل.

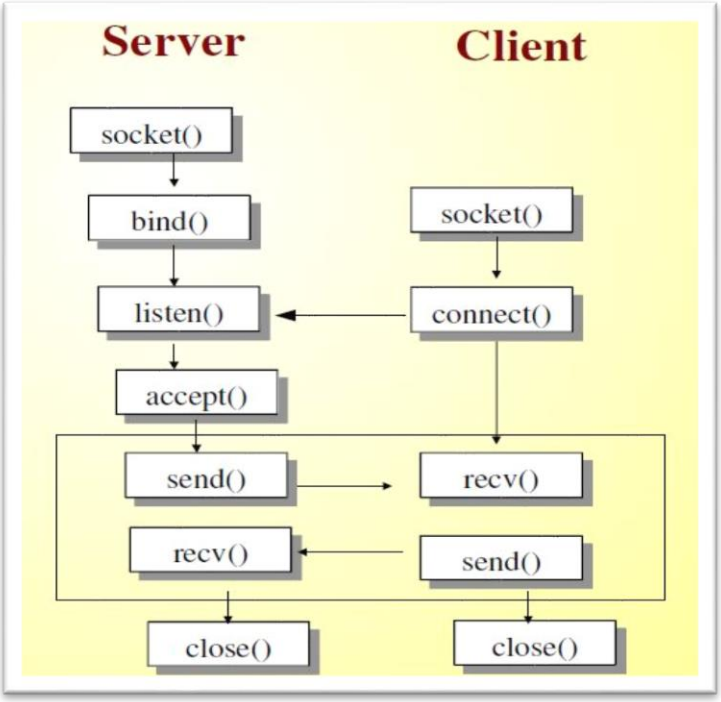
من ناحية أخرى، سيسمح UDP بالاتصال بالبث إلى العديد من العملاء (البث المتعدد).[27]

1.11.2 مقبس الدفق مع بروتوكول مهيأ للاتصال TCP

اتصال TCP عبارة عن قناة ثنائية الاتجاه يتم تحديد نهاياتها بواسطة عنوان IP ورقم المنفذ. قبل استخدامه للاتصال، يجب التفكير في اتصال TCP كمرحلة إعداد، والتي تبدأ مع عملاء TCP الذين يرسلون طلب اتصال إلى خادم TCP.تم تصميم TCP لاكتشاف الخسائر والازدواجية والأخطاء الأخرى التي قد تحدث في قناة مضيف إلى مضيف التي يوفرها IP والاسترداد منها. يوفر بروتوكول TCP قناة تدفق بايت موثوقة، بحيث لا تضطر التطبيقات للتعامل مع هذه المشكلات.

إنه بروتوكول موجه للاتصال، قبل استخدامه للتواصل، يجب أن يقوم برنامجان أولاً بإنشاء اتصال TCP، والذي يتضمن إكمال تبادل رسائل المصافحة بين تطبيقات TCP على جهازي الكمبيوتر المتصلين. يتشابه استخدام TCP أيضًا من نواحٍ عديدة في ملف الإدخال / الإخراج (0/1). في الواقع، يعد الملف الذي يكتبه أحد البرامج ويقرأه برنامج آخر نموذجًا معقولًا للاتصال عبر اتصال TCP.عند قبول طلب الاتصال، يتم إنشاء مقبس بيانات يمكن من خلاله لعملية الخادم الكتابة أو القراءة من / إلى تدفق البيانات. عند انتهاء جلسة الاتصال بين العمليتين، يتم إغلاق مقبس البيانات وتكون عملية الخادم مجانية لقبول طلب اتصال آخر.

يوضح الشكل التالي العلاقة بين العميل / الخادم لواجهة برمجة تطبيقات مآخذ التوصيل لبروتوكول مهيأ للاتصال.الشكل 6.2 يوضح خوارزمية مأخذ التوصيل TCP[20]



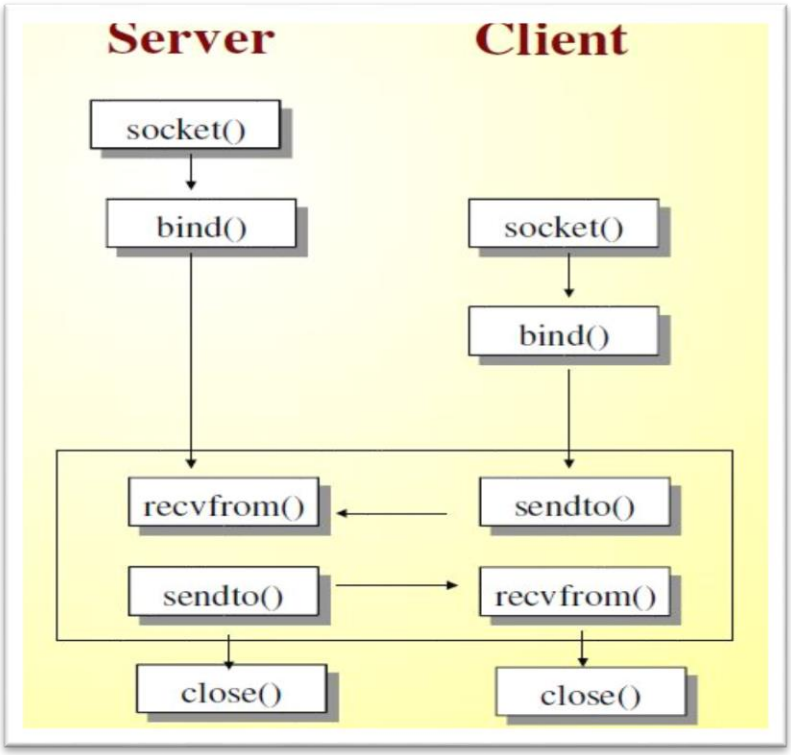
الشكل 6.2: خوارزمية مـأخذ التوصيل TCP

2.11.2 بروتوكول مخطط بيانات المستخدم UDP

المقابس غير المتصلة (بروتوكول مخطط بيانات المستخدم أو UDP) هي خيارك الآخر لنقل البيانات بين جهازين متصلين بالشبكة. تُستخدم عادةً في التطبيقات التي تتطلب القليل من النفقات العامة والتي تريد تحقيق إنتاجية أعلى للشبكة، مثل بروتوكولات دفق الوسائط المتعددة. ميزة أخرى في استخدام UDP هي أنه قادر على نقل البيانات إلى نقاط نهاية متعددة في وقت واحد لأن الاتصال غير مرتبط بعنوان واحد.

نظرًا لأن UDP ينقل مخططات البيانات (حزم الرسائل) بدلاً من دفق متصل، تعتبر هذه الاتصالات غير موثوقة وغير متصلة. ومع ذلك، لا نخطئ في المصطلح غير موثوق لا يقصد به الجودة المنخفضة لكن يعني فقط أن البروتوكول لا يضمن وصول حزم البيانات الخاصة بك إلى وجهتك. علاوة على ذلك، لا يوجد ترتيب تسلسلي يضمن وصولها، ولا أي إخطار إذا لم تصل الحزمة مطلقًا. يوفر مقبس مخطط البيانات واجهة اتصال بدون اتصال. بموجب هذا النموذج، لا تحتاج عمليات الاتصال إلى إعداد اتصال قبل تبادل الرسائل. بدلاً من ذلك، يحدد المرسل عنوان الوجهة في كل رسالة. لا يوجد أي ضمان بأن المستلم سيكون جاهزًا لتلقي الرسالة ولن يتم إرجاع أي خطأ إذا تعذر تسليم الرسالة.[24]

يتم إرسال الرسائل واستلامها باستخدام مكالمات النظام send to وrecvfrom. يتم إنشاء مآخذ مخطط البيانات كما كان من قبل. إذا كانت هناك حاجة إلى عنوان محلي معين، فيجب أن تسبق عملية الربط عملية نقل البيانات الأولى. خلاف ذلك، سيقوم النظام بتعيين العنوان المحلي و / أو المنفذ عند إرسال البيانات لأول مرة.[24]



الشكل 7.2: خوارزمية مـأخذ التوصيل UDP

12.2 أوضاع الاتصال

هناك طريقتان للتواصل بناءً على ما إذا كان يسبقهما فتح اتصال أم لا ويتبعهما إغلاق أم لا.[19]في هذا النموذج يوجد خادم واحد للعديد من العملاء بشكل تعسفي للإجابة على طلباتهم. هناك طريقتان أساسيتان للتواصل عبر الشبكة.

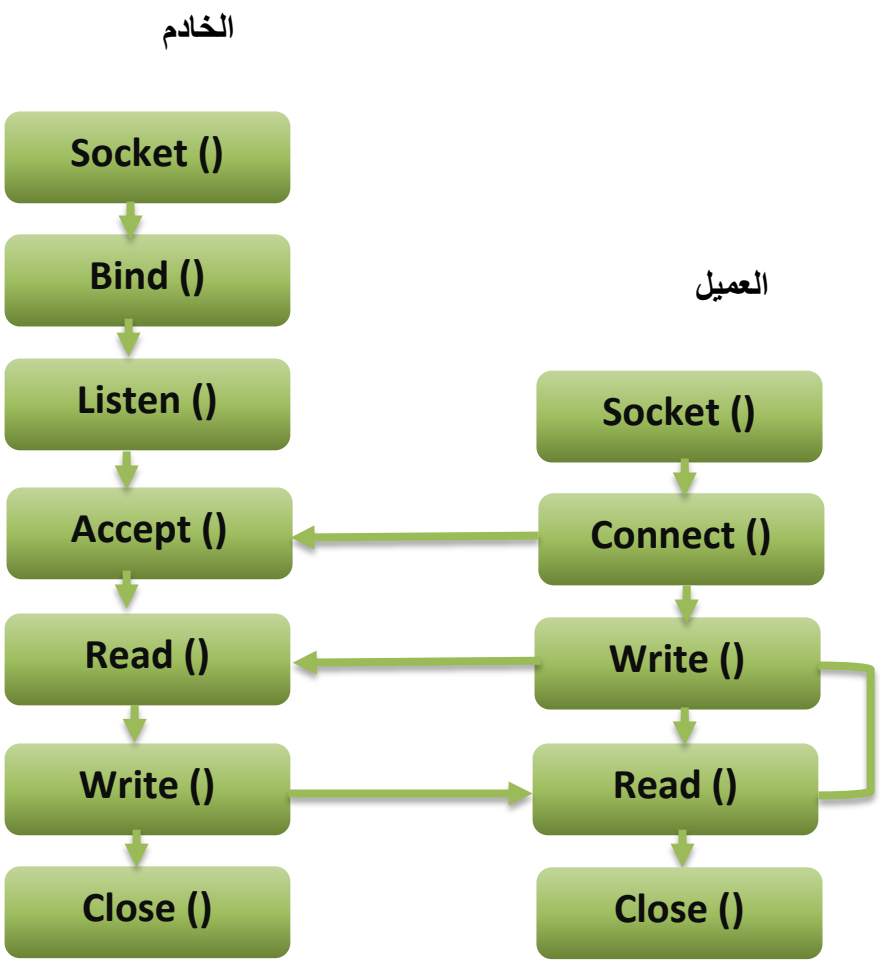
1.12.2 وضع الاتصال

يعد الوضع المتصل هو الطريقة الطبيعية للتعامل مع اتصالات الشبكة، وهو يتوافق بشكل وثيق مع كيفية استخدام الأشخاص للتواصل عبر خط هاتف.

في هذا الوضع، يشترك الطرفان في اتصال (افتراضي) يرسلان البيانات عبره. يجب فتح الاتصال أولاً، ثم يمكن إرسال البيانات وإغلاق الاتصال في النهاية.

إن احتمال ضياع البيانات التي يتم إرسالها بهذه الطريقة ضعيف وستصل دائمًا بالترتيب الذي تم إرسالها به. تعمل كل من شبكة الهاتف التقليدية و TCP للإنترنت بهذه الطريقة.

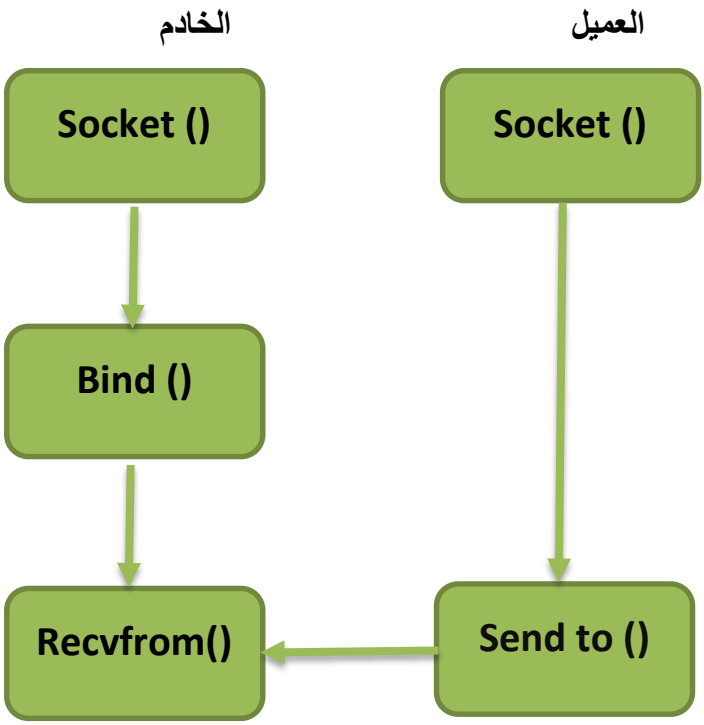
[24] الرسم التخطيطي في الشكل8.2 يوضح الاتصال في الوضع المتصل[20]



الشكل 8.2: الاتصال في الوضع المتصل

2.12.2: وضع الفصل

الوضع غير المتصل هو طريقة اتصال لا يلزم فيها إنشاء اتصال بين الأطراف المتصلة. في هذا الوضع يتم بث المعلومات. نظرًا لعدم وجود فكرة اتصال، لا يمكن اكتشافها إذا لم يتم التقاط المعلومات بواسطة جهاز استقبال أو قد تصل المعلومات خارج الترتيب. يعمل الراديو والتلفزيون وكذلك UDP للإنترنت في هذا الوضع. [24] رسم تخطيطي للاتصال في وضع عدم الاتصال.[20]



الشكل 9.2: الاتصال في وضع عدم الاتصال

13.2 خاتمة

تعتبر المقابس مفيدة لكل من التطبيقات المستقلة والشبكات. تسمح لك المقابس بتبادل المعلومات بين العمليات على نفس الجهاز أو عبر شبكة، وتوزيع العمل على أكثر الأجهزة كفاءة، كما أنها تتيح الوصول بسهولة إلى البيانات المركزية مما يسمح بتبادل البيانات بين جميع أجهزة الشبكة بأريحية وفي وقت أسرع.

الفصل الثالث
التشفير والتأمين

1.3 مقدمة

تم اختراع علم التشفير بهدف تأمين الاتصالات التي يعتبرها المرسل سرية. من الناحية اللغوية، تأتي كلمة التشفير من الكلمة اليونانية "kryptos "والتي تعني إخفاء وكلمة "graphein " التي تعني الكتابة.

يحظى التشفير بمكانة خاصة في علوم أمن المعلومات لما يوفره من سرية لها. وتعرف أهميته والحاجة إليه تزايدا مستمرا يوما بعد يوم وذلك باعتباره لبنة أساسية لأمان الكمبيوتر ودوره في حماية انتقال البيانات الخاصة والسرية من جهاز كمبيوتر إلى آخر دون التلاعب بها واستغلالها.

فاستخدم التشفير عبر التاريخ لتبادل رسائل لا يمكن قراءتها من قِبَل أيا كان ما عدا الشخص المقصود لتلقي الرسالة.

لتأمين الاتصالات في شبكات الحاسوب يتم استخدام أنواع مختلفة من خوارزميات التشفير لتشفير البيانات المتبادلة في الشبكة ومنع أي مستخدم غير مرغوب فيه من قراءة محتوى هذه البيانات وتعديله.

في هذا الفصل، نركز على أهم جوانب مجال التشفير ونعرض نظرة عامة للطرق الكلاسيكية والحديثة لهذا العلم، وأبعاد التشفير.

2.3 تعريف علم التشفير Cryptography

يعطي Le Petit Larousse التعريف التالي: "مجموعة من تقنيات التشفير التي تضمن حرمة النصوص والبيانات في الحوسبة "[28]

في الأساس علم التشفير هو العلم الذي يستخدم المنطق الرياضي لتشفير البيانات و فك تشفيرها للحفاظ على أمان المعلومات حيث يمكن أي شخص من تخزين المعلومات الحساسة أو نقلها بشكل آمن من خلال شبكات غير آمنة (الأنترنت) لمنعها من التعرض القرصنة، التنكر أو التغييرمن قبل أي شخص باستثناء المستلم. [29]

علم التشفير له فرعين: التشفير وتحليل الشفرات.

- **مفهوم التشفيرEncryption**

إن كلمة التشفير مصطلح عام يعين جميع التقنيات المستخدمة لتشفير الرسائل، أي جعلها غير مفهومة بدون إجراء محدد. [30]

يتعامل التشفير مع التأمين الفعلي للبيانات الرقمية، مثل المستندات، الصور أو المعاملات الإلكترونية داخل الإنترنت من الأشخاص غير المرغوب فيهم للحيلولة دون الوصول إليها أو

تغييرها. يعمل التشفير باستخدام شيفرة "صيغة رياضية" ومفتاح لتحويل البيانات المقروءة "نص عادي" إلى شكل لا يستطيع الآخرون فهمه "نص مشفر". [31]

- **مفهوم تحليل الشفراتCryptanalysis**

يُعرف فن وعلم كسر النص المشفر بتحليل الشفرات.

يشير تحليل الشفرات إلى دراسة الأصفار أو النص المشفر أو أنظمة التشفير (أي أنظمة الشفرة السرية) بهدف إيجاد نقاط ضعف في هذه الأنظمة تسمح باسترجاع النص العادي من النص المشفر دون الحاجة إلى معرفة المفتاح أو الخوارزمية. [29] يستخدم تحليل التشفير أيضًا أثناء تصميم تقنيات التشفير الجديدة لاختبار نقاط القوة الأمنية الخاصة بها.

ملاحظة –يهتم علم التشفير بتصميم أنظمة التشفير، بينما يدرس تحليل التشفير كسر أنظمة التشفير.

3.3 الهجمات الأمنية Security Attacks

نميز نوعين من الهجمات الهجوم النشط والهجمات السلبية. فيما يلي نقدم شرح كل نوع على حدى.

1.3.3 الهجمات النشطة Active Attacks

إنه نوع الهجوم الذي يحاول المهاجم فيه تغيير محتوى البيانات مثل تغيير المحتويات. لذلك سيغير المهاجمون الرسالة الأصلية ويعيدون إرسالها إلى المستلم للتظاهر بأنها مرسلة من المرسل المعين.

ويقسم الهجوم النشط الى أربع فئات: التنكر، إعادة العرض، تغيير مضمون الرسائل وانكار الخدمة.

2.3.3 الهجمات السلبية Passive Attacks

إنه نوع الهجوم الذي يقرأ المهاجم فيه فقط المعلومات الدقيقة للرسالة دون أي تعديل عليها.

توجد العديد من الهجمات الأخرى بدلا من المذكورة أعلاه، والتي تحاول كسر خوارزمية التشفير مثل هجوم القوة الغاشمة وما إلى ذلك. [32]

4.3 أبعاد التشفير

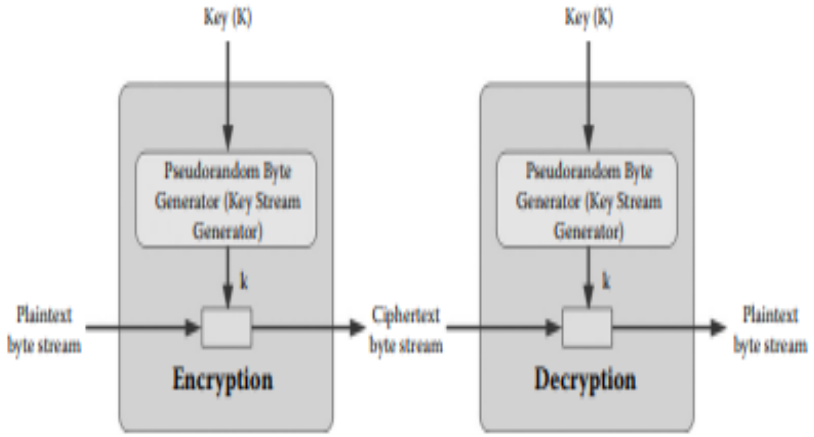
تتميز أنظمة التشفير بثلاثة أبعاد مستقلة:

- نوع العمليات المستخدمة لتحويل نص عادي الى نص مشفر، تستند جميع خوارزميات التشفير الى مبدأين عامين: الاستبدال، حيث يتم تعيين كل عنصر في النص العادي (بت، حرف، مجموعة بتات او أحرف) في عنصر اخر، والتبديل، حيث يتم إعادة ترتيب العناصر في النص العادي.
- عدد المفاتيح المستخدمة. إذا كان كل من المرسل والمستقبل يستخدمان نفس المفتاح، فسيتم الإشارة إلى النظام على أنه متماثل أو مفتاح واحد أو مفتاح سري أو تشفير تقليدي. إذا كان المرسل والمستقبل يستخدمان مفاتيح مختلفة، فيشار إلى النظام على أنه غير متماثل أو تشفير ثنائي أو تشفير المفتاح العام.
- الطريقة التي يتم بها معالجة النص العادي (في حالة تشفير الكتلة او تشفير التدفق).[24]

5.3 تيار الأصفار وكتلة الأصفار

1.5.3 تشفير التدفق Stream encryption

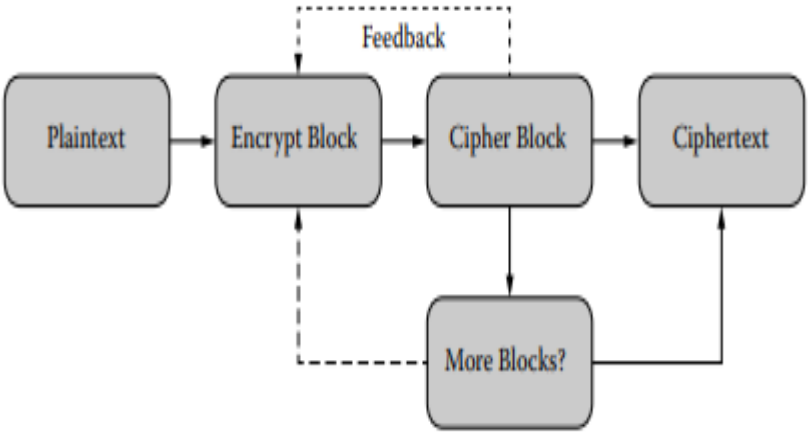
هو طريقة لتشفير النص (لإنتاج نص مشفر) يتم فيها تطبيق مفتاح تشفير وخوارزمية على كل رقم ثنائي في دفق البيانات، بته واحدة في كل مرة. لا تستخدم هذه الطريقة كثيرا في التشفير الحديث. من أمثلة أصفار التيار الكلاسيكي تشفير Vigenere التلقائي وشفرة Vernam.



الشكل 1.3: نموذج مخطط تشغيلي لتشفير التيار

2.5.3 تشفير الكتلة Block Cipher

هو طريقة لتشفير النص (لإنتاج نص مشفر) يكون فيها التشفير بتطبيق المفتاح و الخوارزمية على كتلة من البيانات (على سبيل المثال، 64 بتا متجاورا) في وقت واحد كمجموعة بدلا من بت واحد في كل زمن.[29]



الشكل 2.3: نموذج مخطط تشغيلي لتشفير الكتلة

6.3 تاريخ

1.6.3 التشفير القديم Classic cipher

يعتبر التشفير الكلاسيكي من أقدم أنواع التشفير، حيث بدأ ظهور هذا العلم منذ آلاف السنين ويعتمد هذا التصنيف في أسلوب التشفير على أحد الأمرين أو التقنيتين التاليين:

. **تبديل الأحرف Subtitution** وهو عبارة عن عملية تبديل الأحرف أو الرموز في النص او البيانات المراد تشفيرها لأحرف أو رموز أخرى ومثال ذلك أن يتم تغيير الحرفA للحرف X والحرف B لحرف آخر. وحتى يتم فك تشفير هذه البيانات على الشخص أن يكون على دراية بطريقة تحويل هذه الأحرف.

. **تبديل أماكن الأحرف Transposition** وهي عملية إعادة ترتيب الأحرف والأرقام والرموز في النص أو البيانات المراد تشفيرها ووضعها في مكان مختلف عن مكانها الأصلي في النص أو البيانات فمثلاً يمكن أن تصبح كلمة Technawi بعد التشفير enwcThai .[33]

2.6.3 مقياس سبارتان scytal Spartan

الاستخدام الحقيقي للتشفير كان في القرن الخامس قبل الميلاد في اليونان قديمًا، كان يعتمد على تبديل الحروف. استخدمت مدينة سبارتا عصا ذات قطر معروف، حوله يتم لف شريط مكتوب عليه الرسالة. بمجرد الانتهاء، يتم فك الشريط وبالتالي تصبح الرسالة غير مفهومة. عند الاستلام، يتم لف الشريط حول عصا من نفس القطر كما هو الحال عند الإرسال للحصول على الرسالة الواضحة. تم تصوير كتاب Spartan Scytale بالشكل التالي:

الشكل 3.3: مقياس سبارتان

3.6.3 مربع بوليبيوس polybial square

قبل 150 عامًا من كتابة الكاتب اليوناني جي سي (JC)، أنشأ بوليبيوس عملية تشفير جديدة، التشفير عن طريق الاستبدال. يأتي على شكل جدول من 25 مربع، حيث يحتوي كل مربع على حرف من الحروف الأبجدية مما يعني أن كل حرف يتم تمثيله بزوج من الأرقام التي تشير إلى رقم الصف والعمود في الجدول. بدلاً من إرسال الرسائل في الرسالة، نرسل الأرقام وعند الاستقبال، لدينا نفس الجدول الذي يساعد في فك تشفير الرسالة.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i, j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

الشكل 4.3: مربع بوليبيوس

4.6.3 تشفير قيصر (استبدال أحادي الأبجدي) Caesar Cipher

بعد قرن من الزمان، وبالتحديد في عام 44 قبل الميلاد، ولدت طريقة تشفير، وهي الاستبدال الأبجدي الأحادي. تم استخدامه من قبل يوليوس قيصر، حيث قام بتحويل أحرف الرسائل التي يرسلها إلى جنرالاته بثلاثة أرقام إلى اليمين بالترتيب الأبجدي، على سبيل المثال لإرسال "A"، كتب "D" لإرسال كتب "B"كتب "E" إلخ. عند الاستقبال، تم إزاحة الأحرف بمقدار 3 في الاتجاه المعاكس للأبجدية للحصول على الرسالة.

5.6.3 رمز Vigenere(استبدال متعدد الأبجدية)

في عام 1586، تم اختراع طريقة تشفير أكثر تقدمًا، وهي التشفير عن طريق الاستبدال متعدد الأبجدية. إستنادا إلى تشفير قيصر، تقوم هذه الطريقة بإجراء التحول بكلمة حيث يشير كل حرف إلى التحول الأبجدي المطلوب تطبيقه على النص العادي.

6.6.3 ميكنة التشفير

هي تطوير آلات تقوم بتشفير النص العادي تلقائيًا. نتيجة لذلك، تم اختراع العديد من الآلات.

آلة دي جيفرسون

تقوم هذه الآلة بإجراء التحويل الأبجدي المتعدد تلقائيًا. تشغيله بسيطة، نقوم بتدوير البكرات لتشكيل الرسالة التي نريد إرسالها، ونختار رسالة أخرى موجودة على الاسطوانة. على جانب جهاز الاستقبال، يجب أن يكون لديه نفس الجهاز. لفك الشفرة، يجب عليه تدوير البكرات من أجل صياغة الرسالة المستلمة (المشفرة) ثم يبحث عن الرسالة الواضحة.

أنجما

بدأت قصة آلة أنجما عام 1919، عندما قدم المهندس الهولندي هوغو ألكسندر كوخ براءة اختراع لآلة تشفير كهرو ميكانيكية. تم تبني أفكاره من قبل الدكتور آرثر شيربيوس ، الذي أسس شركة في برلين لتصنيع و تسويق آلة تشفير مدنية: انجما. هذه الشركة فشلت ولكن جذبت آلة إنجما انتباه الجيش. تم كسر تشفيرها من قبل فريق بولندي (ماريا نريجوسكي) في عام 1933. تم تعزيزه من قبل الألمان لاستخدامها في الحرب العالمية الثانية قبل أن يتم كسرها مرة أخرى بواسطة قنابل تورينج.

7.3 التشفير الحديث

أدى ظهور الكمبيوتر إلى تحويل المعلومات إلى سلسلة من البتات (1 و 0)، مما سهل معالجتها و التلاعب بها، أدى هذا إلى ظهور عمليات تشفير جديدة تقدم خوارزميات معقدة بشكل متزايد بمفاتيح ذات حجم هائل.

لا تزال تستخدم حتى اليوم وتتطور كل يوم. هذه الخوارزميات سيتم مناقشتها لاحقًا في هذا الفصل. [34]

1.7.3 الخدمات الأمنية لأمن المعلومات

الهدف الأساسي من استخدام التشفير هو توفير خدمات أمن المعلومات الأساسية التالية. دعونا الآن نرى الأهداف المحتملة التي يقصد تحقيقها بالتشفير.

- **المصادقة Authentication**

تعني عملية التحقق من هوية الكيانات التي تتواصل عبر الشبكة.

بدون المصادقة، يمكن لأي مستخدم لديه وصول إلى الشبكة استخدام الأدوات المتاحة بسهولة لتزوير عناوين بروتوكول الانترنيت(IP) الاصلية وانتحال شخصية الآخرين. لذا، تستخدم أنظمة التشفير آليات مختلفة لمصادقة كل من المنشئ والمتلقي للمعلومات. على سبيل المثال أن المستخدم يحتاج إلى إدخال بياناته اسم تسجيل الدخول وكلمة المرور لحسابات البريد الإلكتروني المصادق عليه من قبل الخادم.

- **التفويض Authorization**

هو وظيفة أساسية للأمان لا يمكن أن يوفرها التشفير. يشير التفويض إلى عملية منح أو رفض الوصول إلى مورد أو خدمة الشبكة. بمعنى آخر، بمعنى آخر التفويض يعني التحكم في الوصول إلى أي مورد مستخدم لشبكات الكمبيوتر. معظم أنظمة أمان الكمبيوتر التي نقوم بها اليوم تستند إلى آلية من خطوتين.

الخطوة الأولى هي المصادقة، والخطوة الثانية هي التفويض أو التحكم في الوصول، والذي يسمح للمستخدم بالوصول إلى الموارد المختلفة بناءً على هوية المستخدم. وتستعمل مراقبة حركة البيانات access control list ACL

- **السرية أو الخصوصية privacy or confidentiality**

ويقصد بها التأكيد على ان المستخدمين المصرح لهم فقط هم من يمكنهم قراءة المعلومات

السرية أو استخدامها. بدون السرية، يمكن لأي شخص لديه وصول إلى الشبكة استخدام

الأدوات المتاحة بسهولة للتنصت على حركة مرور الشبكة واعتراض معلومات الملكية القيمة.

إذا كانت الخصوصية أو السرية غير مضمونة، فقد يسرق الغرباء أو المتطفلين المعلومات المخزنة في نص عادي. ومن ثم، فإن أنظمة التشفير تستخدم تقنيات مختلفة وآليات لضمان سرية المعلومات.عند استخدام مفاتيح التشفير على نص عادي لإنشاء نص مشفر، يتم تعيين الخصوصية للمعلومات.

- **النزاهة Integrity**

هي الجانب الأمني الذي يؤكد أن المحتويات الاصلية للمعلومات لم يتم تغييرها أو إتلافها. إذا لم يتم ضمان النزاهة، فقد يقوم شخص ما بتغيير المعلومات أو المعلومات قد تتلف، وقد لا يتم اكتشاف التغيير في بعض الأحيان. هذا هو السبب في أن العديد من أنظمة التشفير تستخدم تقنيات وأنماط ميكانيكية للتحقق من سلامة المعلومات.

على سبيل المثال، قد يغير المتسلل ملفا سرا، ولكنه يغير بصمة الإبهام الرقمية الفريدة للملف، مما يتسبب في قيام مستخدمين آخرين باكتشاف التلاعب من خلال مقارنة بصمة الإبهام الرقمية المتغيرة ببصمة الإبهام الرقمية للمحتويات الأصلية.

- **عدم الإنكار Non-repudiation**

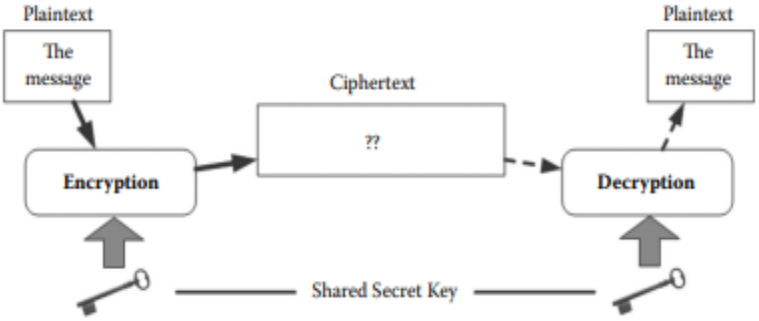
لتوصيل المعلومات، هناك حاجة الى ضمان ان الطرف لا يمكنه انكار خطا ان جزءا من الاتصال الفعلي قد حدث. يضمن عدم الانكار ان كل طرف مسؤول عن رسالته المرسلة. إذا لم يتم ضمان عدم الانكار، يمكن لأي شخص التواصل ثم فيما بعد اما ان ينكر الاتصال كاذبا تماما او يدعي انه حدث في وقت مختلف او حتى ينكر تلقي أي معلومة. ومن ثم فان هذا الجانب يضمن مساءلة كل كيان يشارك في حدث الاتصال. [29]

8.3 أنواع التشفير الحديث

في مجال التشفير الحديث، هناك طريقتان أساسيتان للتشفير: التشفير المتماثل والتشفير غير المتماثل.

1.8.3 التشفير المتماثل Symmetric encryption

يُعرف هذا التشفير أيضًا باسم تشفير المفتاح الخاص. يكون المفتاح المستخدم لتشفير النص العادي هو نفسه المستخدم لفك تشفير النص المشفر، مما يجعل هذا الأسلوب الأفضل للمستخدمين الفرديين والأنظمة المغلقة. وبخلاف ذلك، يجب إرسال المفتاح إلى المتلقي وهو ما يزيد من خطر التعرض للاختراق إذا اعترضته جهة خارجية مثل المتسللين. لكن هذه الطريقة أسرع من الطريقة غير المتماثلة.
تتميز خوارزمية التشفير المتماثل بخوارزمية مفتوحة وكمية صغيرة من الحساب وسرعة تشفير وكفاءة تشفير عالية. [35]



الشكل 5.3: النموذج التشغيلي للتشفير المتماثل

مبدأ التشغيل

لنقل رسالة مشفرة بين طرفين A وB باستخدام خوارزمية تشفير متماثل، من الضروري أن يكون لدى A وB المفتاح السري المشترك K.

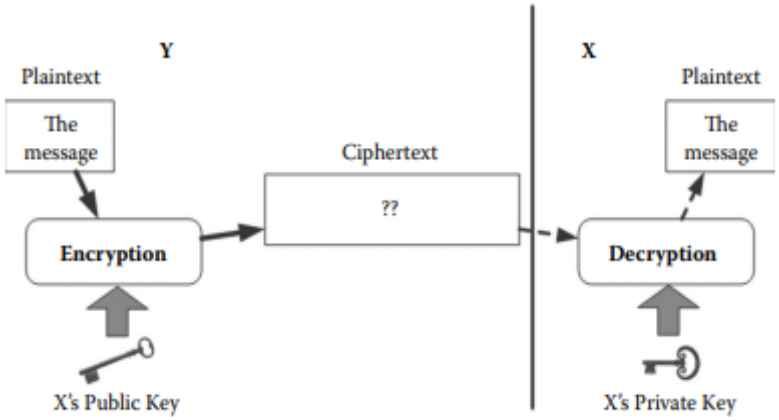
من الناحية العملية، تم منح هذا المفتاح المشترك لكلا الطرفين مسبقًا، أو تم اشتقاقه باستخدام خوارزمية غير متماثلة.

تحتوي خوارزميات التشفير المتماثل على مفاتيح قصيرة80 أو 128 أو 256 بت وأداؤهم مرتفع بشكل عام لذلك يتم استخدامها دائمًا تقريبًا في تشفير البيانات المراد حمايتها. على سبيل المثال، لإرسال بريد إلكتروني آمن يتم استخدام تشفير المفتاح العام فقط لتشفير المفتاح المختار عشوائيًا والذي يشفر جميع البيانات باستخدام خوارزمية متماثلة. [34]

هناك العديد من الخوارزميات من هذا النوع مثل DES وAES وما إلى ذلك. تستخدم كل خوارزمية طريقة مختلفة لتشفير البيانات وفك تشفيرها، سيتم أيضًا تشفير كل منها وفك تشفير حجم ثابت من البيانات ككتلة وحجم ثابت للمفتاح. سيسمح هذا النوع من الخوارزميات فقط بإدخال الحروف الهجائية الإنجليزية والرموز الخاصة والقيم الرقمية كنص عادي. لذلك سيتم إنتاج المخرجات (نص مشفر) كمستند في شكل أحرف خاصة أو أبجديات أو أرقام أو دمجها جميعًا.[32]

2.8.3 التشفير غير المتماثل (Asymmetric encryption)

يشير تشفير المفتاح العام والمعروف أيضا باسم التشفير غير المتماثل إلى خوارزمية تشفير تتطلب مفتاحين منفصلين أحدهما سري (أو خاص) والآخر عام. على الرغم من اختلافهما فإن جزأين من زوج المفاتيح هذا مرتبطان رياضيا[29]. يوضح الشكل خطوات التشفير غير المتماثل



الشكل6.3: النموذج التشغيلي لتشفير غير المتماثل

مبدأ التشغيل

يعتمد التشفير غير المتماثل على وظائف أحادية الاتجاه. هذا يعني أن البيانات المشفرة بالمفتاح العمومي لا يمكن فك تشفيرها إلا إذا كان لدى المرء المفتاح السري. هذا يعني أنه حتى لو حصلنا على المفتاح العام، فلن نتمكن من ذلك فك شفرة المعلومات. [34]

9.3 معيار التشفير المتماثل (Data Encryption Standard DES)

في 15 مايو 1973، أصدر المكتب الوطني الأمريكي للمعايير (المعروف الان باسم المعهد

الوطني للمعايير والتكنولوجيا، او NIST)، مناقصة نظام التشفير في " معيار تشفير البيانات " او DES في السجل الفيدرالي، وتم الاحتفاظ به وأصبح نظام التشفير الأكثر انتشارا في العالم.

طورت IBM في الأصل DES لتعديل نظام سابق يسمى "LUCIFER" تم نشر DES في السجل الفيدرالي في 17 مارس 1975. بعد نقاش عام كبير، تم اعتماده كمعيار للتطبيقات غير المصنفة في 15يناير 1977. منذ اعتمادها تمت إعادة تقييم DES من قبل المكتب الوطني للمعايير كل ما يقرب من خمس سنوات. يعود تاريخ أحدث مراجعة إلى يناير 1999؛ في ذلك الوقت كان تطوير خليفته AES قد بدأ بالفعل. [36]

معيار تشفير البيانات DES، هو خوارزمية تشفير متماثل (تشفير كتلة) باستخدام مفاتيح 56 بت. لم يعد استخدامه موصى به اليوم بسبب تنفيذه البطيء ومساحته الرئيسية الصغيرة جدًا مما يسمح بهجوم منظم في وقت معقول. عندما لا يزال قيد الاستخدام يكون عادةً في Triple DES، والذي لا يفعل شيئًا لتحسين أدائه. تم استخدام DES بشكل ملحوظ في نظام كلمة مرور UNIX.[37]

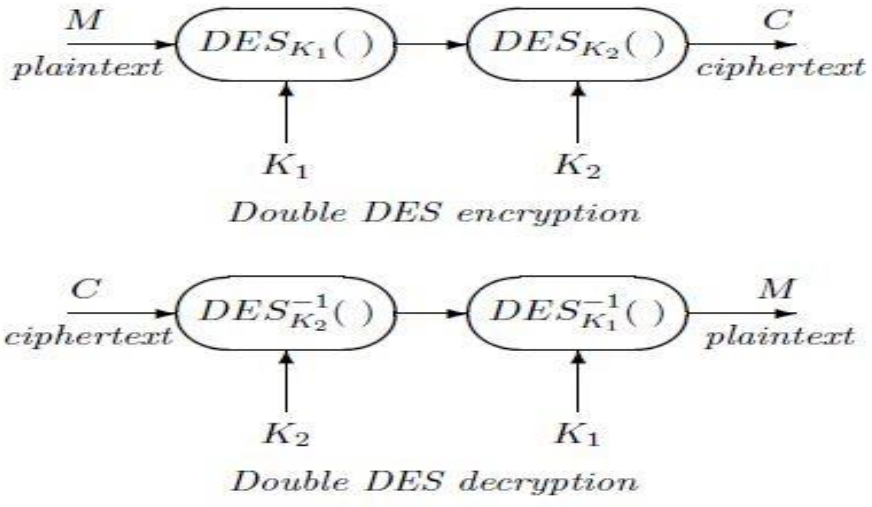
1.9.3 تشفير DES المتعدد (Multiple DES encryption)

باستخدام أكثر من مفتاح واحد يوفر تشفير DES المتعدد قوة تشفير إضافية ل DES

نعرض فيما يأتي كيفية حماية المعلومات باستخدام DES المزدوج والثلاثي.

تشفير DES المزدوج (Double DES encryption)

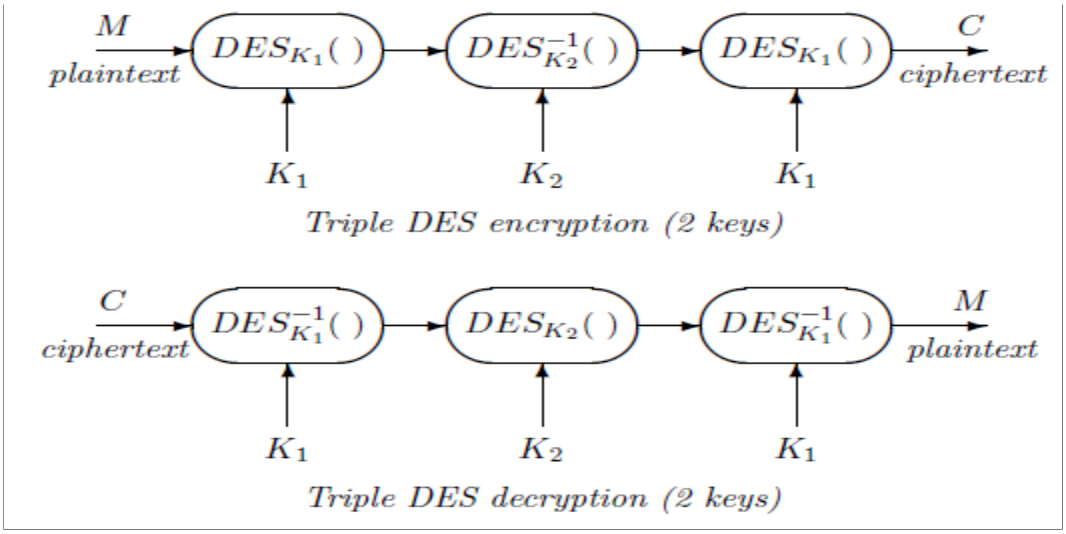
يتم تحقيق تشفير DES المزدوج لرسالة نص عادي من خلال تطبيق تحويل تشفير DES على الرسالة باستخدام مفتاح 56 بتK1 ثم تطبيق تشفير DES على كتلة 64 بت الناتجة مع مفتاح 56 بت ثاني K2 ، فك تشفير النص المشفر يتم الحصول على DES المزدوج عن طريق تطبيق تحويل فك تشفير DES مرتين أولا مفتاح الثاني K2 ثم K1 ، والشكل 7.3 يوضح عمليات التشفير وفك التشفير DES المزدوجة



الشكل7.3: التشفير المزدوج وفك التشفير

- **تشفير DES ثلاثي الابعاد (Triple DES encryption)**
  - **تشفير DES الثلاثي مع مفتاحين**

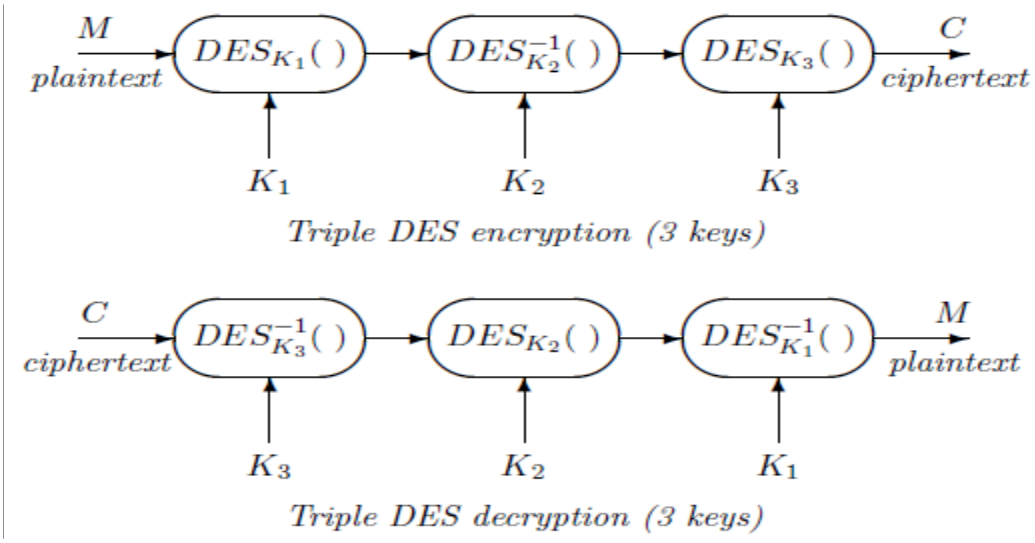
لمنع هجوم في النوع الأوسط meet– in –the– middle، يمكن استخدام مربع تشفير DES ثالث في سلسلة مع مفتاحين مميزين k1 k2 كما هو موضح في الشكل 8.3 يتم إجراء تشفير و فك تشفير DES الثلاثي باستخدام مفتاحين مختلفين على النحو التالي:



الشكل8.3: التشفير الثلاثي وفك التشفير باستخدام مفتاحين

- **تشفيرDESالثلاثي مع 3 مفاتيح Triple DES encryptions with 3 keys**

الثلاثي مع ثلاثة مفاتيح مختلفة حتى إذا لم تكن هناك طريقة **DES**لا يزال البعض يفضل استخدام تشفير ثلاثي مع مفتاحين. يوضح الشكل التالي طريقة عمل هذا التشفير.[38]DESمعروفة لكسر تشفير



الشكل9.3: تشفير DES الثلاثي وفك التشفير باستخدام 3 مفاتيح مختلفة

10.3 معيار التشفير المتقدم Advanced Encryption Standard AES

في يناير 1997، بدأت NISTعملية لاستبدال DES الى معيار التشفير المتقدم(AES). تم اصدار RFP رسمي في 12 سبتمبر 1997 تطلبت AES ان يكون لها حجم كتلة يساوي 128 بت وذلك انه يدعم اطوال مفاتيح تساوي 128 و192 و256 بت، ويجب ان تكون AES خالية من حقوق الملكية في جميع انحاء العالم.

كان موعد التقديم في 15 يونيو 1998. من أصل واحد وعشرين نظام تشفير تم تقديمه، استوفى خمسة عشر جميع المعايير اللازمة وتم قبولهم كمرشحين ل AES. قدمت NISTالمرشحين الخمسة عشر ل AES في المؤتمر الأول لمرشحي AES في مارس 1999. في أغسطس 1999 تم اختيار خمسة مرشحين من قبل NISTكمرشحين نهائيين: MARS،RC6، RIJNDAEL ، SERPENT وسمكتان. في ابريل 2000، تم

عقد المؤتمر الثالث لمرشح AES. في 2 أكتوبر 2000، تم اختيار RIJNDAEL كمعيار تشفير متقدم. في 28 فبراير 2001، أعلنت NIST ان مسودة معيار معالجة المعلومات الفيدرالية ل AES كانت متاحة للجمهور. تم اعتماد AES كمعيار في 26 نوفمبر 2001 وتم نشره باسم FIPS 197في السجل الفيدرالي في 4 ديسمبر 2001. من الجدير بالذكر ان عملية اختيار AES تمت بطريقة مفتوحة تماما ودولية. قدمت المؤتمرات الثلاثة جنبا الى جنب مع الدعوات للتعليق العام فرصة كبيرة للمناقشة العامة وتحليل المرشحين وقد لقيت العملية استحسانا كبيرا من قبل جميع المشاركين. يتم توضيح الجانب الدولي ل AES من خلال مجموعة متنوعة من البلدان التي يمثلها مؤلفو الخوارزميات الخمسة عشر المرشحة: استراليا، بلجيكا، كندا، كوستاريكا، فرنسا، المانيا، اليابان، كوريا، النرويج والمملكة المتحدة والولايات المتحدة.

- **معيار التشفير المتقدم Rijndael**

Rijndael، التي تم اختيارها كمعيار تشفير متقدم، اخترعها باحثان بلجيكيان Daemen و Rijmen . اصالة أخرى، المؤتمر الثاني لمرشح AES الذي عقد خارج الولايات المتحدة، في روما إيطاليا.

تم تقييم مرشحي AES لامتثالهم للمعايير الرئيسة الثلاثة التالية:

- الأمان
- استرجاع
- خصائص الخوارزمية وتطبيقاتها.

كان امان الخوارزميات المقترحة ضروريا للغاية وأي خوارزمية بها نقاط ضعف امنية سيتم التخلص منها.

التكلفة تشير الى الكفاءة من حيث العمليات الحسابية (متطلبات السرعة والذاكرة) على أنواع مختلفة من المنصات، سواء في البرامج او الأجهزة او على البطاقة الذكية. تشمل "خصائص الخوارزمية وتنفيذها "مرونة الخوارزمية وبساطتها "، من بين معايير أخرى.

في النهاية، وقد شعر جميع المتأهلين للتصفيات النهائية بأنهم امنون. تم اختيار Rijndael لان خصائصها من حيث السلامة، الأداء، الكفاءة، سهولة التنفيذ والمرونة تم الحكم عليها بانها متفوقة على تلك الخاصة بالمتسابقين النهائيين الاخرين.

- **وصف AES**

كما ذكرنا سابقا يبلغ طول كتلة AES 128 بت ولها ثلاثة اطوال مفاتيح محتملة، وهي 128و 192 و256 بت.

AES هي خوارزمية تشفير متكررة ؛ يعتمد عدد المراحل التي يشير اليها Ne على طول المفتاح.

Ne = 10 اذا كان المفتاح بطول 128 بت.

Ne = 12 في حالة مفتاح بطول 192 بت.

Ne = 14 اذا كان المفتاح يحتوي على 256 بت.

نقدم وصفا موجزا ل AES تعمل الخوارزمية على النحو التالي:

1 بالنسبة إلى النص العادي X نقوم بتهيئة الحالة لإجراء عملية ADD ROUNDKEY وتنفيذها والتي تجمع بين Roundkey عن طريق أمر حصري OR مع State

2 لكل مرحلة من مراحل Ne −1، نقوم بإجراء عملية استبدال تسمى" SUBBYTES On State" باستخدام S –box ثم يتم اجراء تبديل SHIFTROWS على الحالة ثم نقوم بإجراء التقليبMIX COLUMNS على الحالة ثم قم بإجراء عملية ADDROUNDKEY.

3 نقوم بتنفيذ SUBBYTES ثم SHIFTROWS وأخيرا ADDROUNDKEY.

4 نحدد النص المشفر ليكون حالة. [36]

11.3 RSA

تم اختراع تشفير RSA في عام 1977 من قبل علماء الرياضيات Ronald Rivest، Adi Shamir و Leonard Adelman أعطت الأحرف الأولى من اسمهم RSA. يعتمد عملها على صعوبة تحليل الأعداد الأولية الكبيرة جدًا. يستخدم على نطاق واسع في جميع أنحاء العالم. في الواقع، هو من بين أشياء أخرى التشفير المستخدم أثناء الاتصالات الآمنة على مستعرض الويب. مع كل مستخدمي الأنترنيت سيكون من المستحيل تخيل استخدام التشفير المتماثل. ولهذا السبب يتم حساب المفتاح الخاص باستخدام RSA.

نظرا لأن الخوارزميات غير المتماثلة أبطأ من الخوارزميات المتماثلة، فإن RSA تحسب فقط المفتاح الذي سيتم استخدامه لتشفير البيانات باستخدام تشفير متماثل مثل AES.

- **مبدأ نظام التشفير RSA**

لإنشاء المفتاح العام الذي يتكون من الرقمين n و e، يجب أن نختار اثنين من الأعداد الأولية كبيرين جدًا p و q بحجم لا يقل عن 2^{512} بت لكل منهما من أجل تكوين مفتاح من 2^{1024} بت ليكون آمنًا بدرجة كافية

التالي، سيتعين علينا حساب n الذي يساوي p * q. يجب ، بعد ذلك حساب φ (n) = (p−1) * (q−1) ، مما سيجعل من الممكن حساب مفتاح فك التشفير d . ثم علينا أن نختار الأس e وهو عدد أولي مع φ(n).

سيتكون المفتاح العمومي من e و n. بالتالي سيكون الطرف الآخر قادرا بفضل e و n على تشفير رسالة بالحساب التالي: $m^e \ mod \ n$. بعد ذلك، لحساب مفتاح فك التشفير، من الضروري أن يكون e * d mod φ(n) = 1. باختصار، للعثور على d، يجب أن نقوم بالحسابات التالية:$e^{-1}\text{mod } \varphi(n)$ للعثور على هذه النتيجة، يمكن استخدام خوارزمية إقليدس الموسعة.

لنأخذ كمثال p = 7، q = 11. لحساب n، يجب علينا ضرب p وq، أيهما يعطينا n = 77. لحساب φ (n)، يجب أن نحسب (7−1) * (11−1) وهو ما يعطينا 60.

الآن، يجب أن نختار الأس e، الذي يجب أن يكون عددًا أوليًا مع φ (n). لذلك دعونا نأخذ على سبيل المثال e = 13 (PGCD (13, 60) = 1 وبالتالي أوليين فيما بعض) إذن هنا المفتاح العمومي = e = 13 et n = 77 للتحقق من صحة d، يكفي حساب e * d mod φ (n) = 1. في هذا المثال هذا يعادل حساب 13 * 37 mod 60 = 1. [28]

12.3 تجزئة SHA−1

تجزئة SHA−1 خوارزمية التجزئة الآمنة تم تطوير وظيفة تجزئة Sha−1 (خوارزمية التجزئة الآمنة) بواسطة NIST في عام 1995. يستخدم SHA−1 كتل 512 بت وينتج رسائل مجزأة 160 بت. تنقسم الكتل إلى 16 كتلة فرعية مكونة من 32 بت لكل منها. ثم يتم تمديدها إلى 80 كتلة. لإنتاج 80 قطعة ننفذ العمليات 4 التالية 80 مرة.

1. F = (B AND C) OR (¬ (B) AND D)
2. F = B XOR C XOR D
2. F = (D AND C) XOR (B AND D) XOR (C AND D)
4. F= B XOR C XOR D

حتى الآن، SHA−1 قابل للكسر نظريا بالقوة الغاشمة. ومع ذلك، فإنه لا يزال من الصعب كسره بسهولة. يمكن العثور بسهولة على كلمة مرور بسيط من النوع "12345" مجزأ باستخدام SHA−1. من ناحية أخرى، كلمة مرور تحتوي على أحرف عشوائية ستستغرق وقتا أطول بكثير للعثور عليها. على الرغم من ذلك، لا يزال يستخدم على نطاق واسع. [28]

13.3 خاتمة

الغرض الأساسي من التشفير هو حماية سرية البيانات الرقمية المخزنة على أنظمة الكمبيوتر أو المنقولة عبر الإنترنت أو أي شبكة كمبيوتر أخرى.

في هذا الفصل، قمنا بعرض المعنى العالمي للتشفير ومفاهيمه الأساسية إضافة الى التعريف بالخوارزميات الكلاسيكية مع ذكر أنواع الاصفار ومناقشة طرق التشفير الحديثة و تطورها حتى وصلنا إلى أحدث طرق التشفير الحالي معيار التشفير المتقدمAES .

الفصل الرابع
تطبيق

1.4 مقدمة

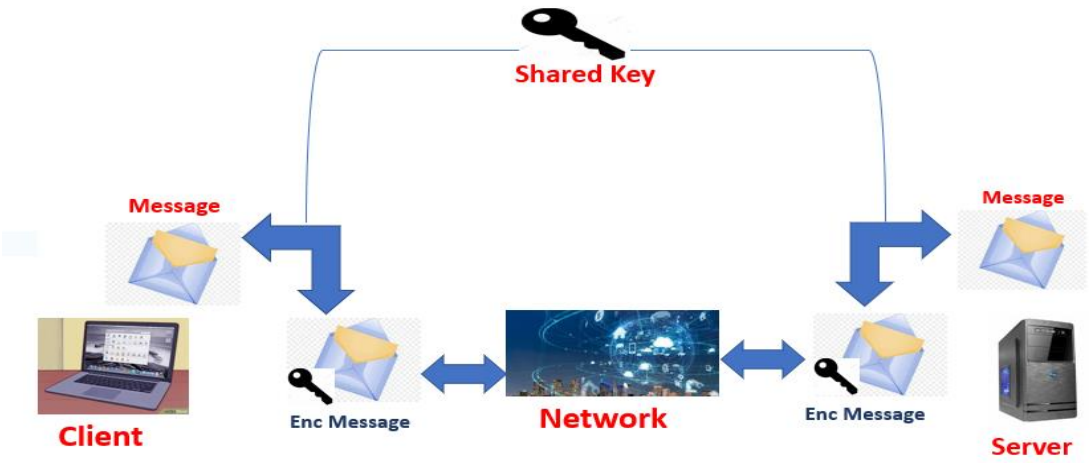
في الفصول الثلاثة السابقة قد تطرقنا الى نموذج الخادم/العميل والمقابس وخوارزميات التشفير المختلفة من قديمة وحديثة الى أن وصلنا الى تشفير AES حيث أن الهدف الأساسي من هذا المشروع هو دمج كل هذه المفاهيم في تجربة أو برمجة مفيدة متمثلة في تنفيذ التشفير المتقدم وفكه عند التواصل بين الخادم والعميل باستخدام المقابس ومن هنا نقول إن هذا الفصل عبارة عن تجميع ما رأيناه سابقا من خلال انشاء نموذج الخادم/العميل وتطبيق عليه خوارزمية التشفير AES لقوتها وكفاءتها من أجل تحقيق هدف هذا المشروع.

2.4 نظرة عامة

بالنسبة لموضوعنا فلقد اخترنا نموذج الخادم/ العميل لدراسته والتعمق في كيفية عمله والذي يعتبر برنامج هندسة برمجية ينقسم إلى نظامين، نظام الخادم ونظام العميل حيث أن هذا البرنامج يقسم المهام بين الخوادم والعملاء والتي تقع إمّا في نفس النظام أو تتواصل من خلال شبكة الكمبيوتر أو الانترنت.

تبادل المعلومات والبيانات في هذا البرنامج تكون أغلبها عبر قنوات اتصال مفتوحة أي غير آمنة وجب علينا هنا التفكير في حمايتها و تأمينها من خطر السرقة و التجسس وهنا نكون قد وصلنا إلى ما يسمى بالتشفير الذي أهميته تزداد مع زيادة أهمية المعلومات و سريتها، حيث أن هذا الأخير هو عملية تحويل البيانات إلى تسلسل من البايت باستخدام احدى خوارزميات التشفير التي درسناها سابقا. والهدف منها هو تأمين المعلومات لكي لا يتسنى الوصول إليها إلا للأشخاص المطلوبين.

وهنا سوف نظهر كيفية عمل نظام الخادم /العميل من خلال الوثيقة التالية التي توضح لنا أنه عند ارسال طلب من العميل إلى الخادم أو الاتصال به فإنه يقوم بإرسال جميع الملفات المطلوبة والتي يستقبلها الخادم ويقوم بتخزينها، وهنا يقوم العميل بتشفير هاته المعلومات أو الملفات وارسالها عبر الشبكة إلى الخادم الذي يقوم بدوره بفك تشفيرها.



الشكل1.4: نموذج الخادم/العميل في تبادل الرسائل

3.4 نظرة مفصلة

في هذا الجزء من العمل سنناقش بدقة أكثر ما يجعل هذا البرنامج محميا وفعالا اكثر، والذي يعتمد هنا عن ثلاثة أجزاء مهمة هي تصميم التطبيق ونقل البيانات وتشفير البيانات.

1.3.4 فوائد بنية الخادم/العميل

_التعامل مباشرة بين الخادم والعميل.

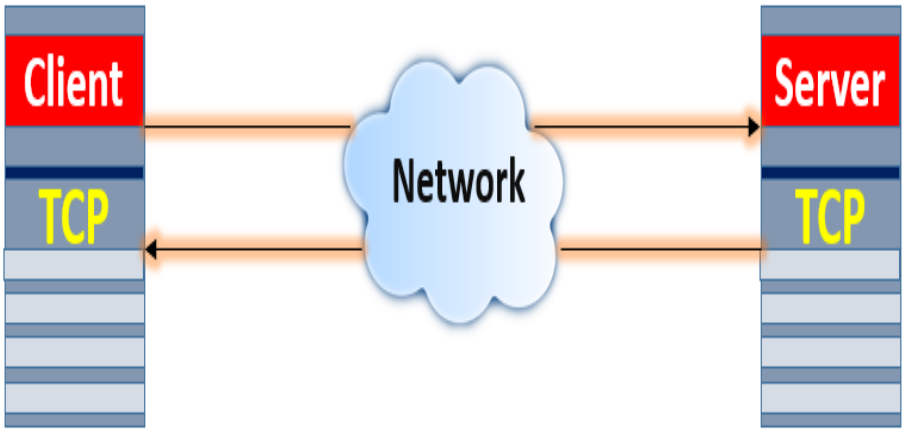
_سرعة الاتصال.

_سهولة التنفيذ.

2.3.4 ضمان تسليم المعلومات

الأمر يتعلق بضرورة حماية وضمان تسليم المعلومات أيا كانت صور أو مستندات أو غيرها، وفي هذه الحالة نكون قد اخترنا الوضع المتصل.

وضع TCP هو ما نعمل به عند توصيل جهازين مع بعض من أجل الاتصال فيما بينهم بشكل مباشر، حيث يقومان بإنشاء رابط افتراضي قبل نقل البيانات، حيث أنه يضمن نقل البيانات بموثوقية وذلك بفضل أنهما يعملان أو يتزامنان في وقت الاتصال وبالتالي فإن العملية تكون نتيجتها مضمونة من حيث إذا كانت البيانات المرسلة تم استلامها فعلا. في حالة عدم استلام المعلومة أو استلامها بشكل خاطئ يرجع الطرف الثاني رسالة خطأ وهنا تقوم TCP بدورها المتمثل في جمع وفرز الحزم، وفي هذه الحالة سيقوم المتلقي بطلب إعادة إرسال.



الشكل 2.4: نموذج بسيط للوضع المتصل

3.3.4 تأمين البيانات باستخدام تشفير AES

معيار التشفير المتقدم (AES) عبارة عن تشفير كتلة متماثل تختاره حكومة الولايات المتحدة لحماية المعلومات السرية. يتم تطبيق AES في البرامج والأجهزة في جميع أنحاء العالم لتشفير البيانات الحساسة. إنه ضروري لأمن الكمبيوتر الحكومي والأمن السيبراني وحماية البيانات الإلكترونية.[38]

4.3.4 كيفية عمل AES

الميزة الاولى لهذا التشفير أو سبب اعتماده هو سهولة تنفيذه في كل من الأجهزة والبرامج، حيث أنه يعمل بالبايت مما يجعل التنفيذ والشرح سهلان. [24] إنه يعمل عن طريق تكرار نفس الخطوات المحددة عدة مرات، و المسماة بالجولات. تتكون كل جولة من عدة خطوات معالجة، بما في ذلك خطوة تستخدم مفتاحًا فرعيًا للتشفير / فك التشفير يتم إنشاؤه من المفتاح المشترك. [39]

5.3.4 المبادئ الأساسية ل AES

هناك مبدأين أساسيان للتشفير المتقدم هما

جيم شانون أظهر C.Shannon أن الجمع بين الارتباك والانتشار جعلت من الممكن الحصول على الضمان المناسب:

- **الارتباك Confusion** = إخفاء أي علاقة خطية بين النص المشفر والرسالة واضح.
- **الانتشار Diffusion** = إخفاء التكرار عن طريق نشر تأثير بت رئيسي على كل التشفير.[40]

هناك ثلاث نسخ للتشفير المتقدم: بالنسبة لهذا التشفير فيتم تنفيذها وتنفيذ عملياته على مصفوفة ثنائية الأبعاد من البايت bytes تسمى الحالة states دائما ما تتكون من 4 صفوف وعدد محدد من الأعمدة يختلف حسب طول المفتاح ففي حالة المفتاح 128 بت فيتكون من 4 صفوف و4 أعمدة. والجدول التالي يوضح لنا النسخ أو الأصناف الثلاثة لهذا التشفير مع عدد الاعمدة والجولات. [41]

طول المفتاح Nk	عدد الاعمدة Nb	عدد الجولات Nr
128	4	10
192	6	12
256	8	14

الجدول 1.4 العلاقة بين Nr. Nb. Nk

6.3.4 الهيكل العام للتشفير المتقدم

يتم تخزين المعلومات في مربع أبعاده عبارة عن 4 صفوف و4 أعمدة (4x4)

S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

الجدول 2.4 جدول حالة مفتاح 128 بت AES

كل صندوق أو مربع صغير يحتوي على 1 x8) 128=16octet) [42]

ويعتمد هذا التشفير على 5 خطوات التي سنقوم بشرحها واحدة تلوى الأخرى بالتفصيل.

أ) **الخطوة الأولى**XOR وهي عملية من عمليات المنطق تعطي النتيجة إيجابا أو تنتج بشكل صحيح عندما يختلف المدخلين عن بعضهما أي عندما يكون أحدهما صحح والثاني خاطئ فان النتيجة صحيحة. والجدول التالي هو الجول الخاص بعملية XOR

المدخل		المخرج
0	0	0
0	1	1
1	0	1
1	1	0

الجدول 3.4 عملية XOR

ب) **الخطوة الثانية التعويض** SubByte

حيث يتم في هذه الخطوة التشفير المتقدم بالاستعانة أو باستخدام جدول يسمى S-box

من أجل اجراء التبديل الخاص بالتشفير وأيضا S–box عكسي يستعمل في عملية فك التشفير.وفي هذه العملية يمثل كل بايت برقمين مثلا 52 حيث يمثل الرقم الأول 5 رقم الصف والرقم الثاني 2 رقم العمود من أجل القراءة السهلة من هاته الجداول. وفيما يلي صورة تبرز لنا جدول S–box والأخرى S–box العكسي.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

الشكل 3.4 :جدول S–box

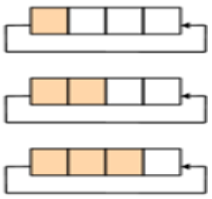
		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

الشكل 4.4: جدول S–box العكسي

ج) الخطوة الثالثة التبديل Rotation

في هذه الخطوة نعتمد على ما يسمى بالإزاحة ويكون بتدوير الصف بعدد ثابت ويكون هذا التحويل نحو اليسار بينما الصف 0 لا يتغير أما الصف الثاني فيزاح ب 1 بايت والصف 2 ب 2 بايت و3 ب 3 بايت وتسمى هذه العملية ب ShiftRows كما هو موضح في الشكل التالي:

S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3



S0,0	S0,1	S0,2	S0,3
S1,1	S1,2	S1,3	S1,0
S2,2	S2,3	S2,0	S2,1
S3,3	S3,0	S3,1	S3,2

الشكل 5.4: عملية ShiftRows

وما ذكرناه الان كان بخصوص التشفير بينما في حالة فك التشفير فيكون العكس أي الازاحة تكون نحو اليمين InvShiftRows

د) الخطوة الرابعة خلط الاعمدة MixColumn

في هذه الخطوة يكون العمل على كل عمود وحده فكل بايت من هذا العمود نقوم بضربه بما يقابله من صف مصفوفة Galois حيث تكون عملية الضرب عمود من المربع مقابل صف من حقل Galois مع عملية XOR على النحو الذي توضحه الصورتان والعمليات التالية المتمثلة في XOR والضرب .

S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

الشكل 6.4: خلط الاعمدة

MixColumn

$$S0,0 = (S0,0*2) \text{ XOR } (S1,0*3) \text{ XOR } (S2,0*1) \text{ XOR } (S3,0*1)$$

$$S1,0 = (S0,0*1) \text{ XOR } (S1,0*2) \text{ XOR } (S2,0*3) \text{ XOR } (S3,0*1)$$

$$S2,0 = (S0,0*1) \text{ XOR } (S1,0*1) \text{ XOR } (S2,0*2) \text{ XOR } (S3,0*3)$$

$$S3,0 = (S0,0*3) \text{ XOR } (S1,0*1) \text{ XOR } (S2,0*1) \text{ XOR } (S3,0*2)$$

هـ) الخطوة الخامسة إضافة مفتاح مستدير AddRounKey

اجراء AddRounKey بسيط للغاية. وهو ينتج من عملية XOR لكل من جدول الحالة St المتكون من 128 بايت و128 بايت من مفتاح التشغيل K .

S0,0	S0,1	S0,2	S0,3
S1,0	S1,1	S1,2	S1,3
S2,0	S2,1	S2,2	S2,3
S3,0	S3,1	S3,2	S3,3

XOR

K0,0	K0,1	K0,2	K0,3
K1,0	K1,1	K1,2	K1,3
K2,0	K2,1	K2,2	K2,3
K3,0	K3,1	K3,2	K3,3

الشكل 7.4: إضافة مفتاح مستدير AddRounKey

7.3.4 هيكل AES

يظهر الهيكل العام لتشفير / فك تشفير AES حسب الشكل.

عدد الجولات 10 عندما يكون مفتاح التشفير بطول 128 بت. (كما ذكر سابقا، عدد الجولات هو 12 عندما يكون المفتاح 192 بت و14عندما يكون المفتاح 256)

بالنسبة للتشفير، تتكون كل جولة من الخطوات الأربع التالية:

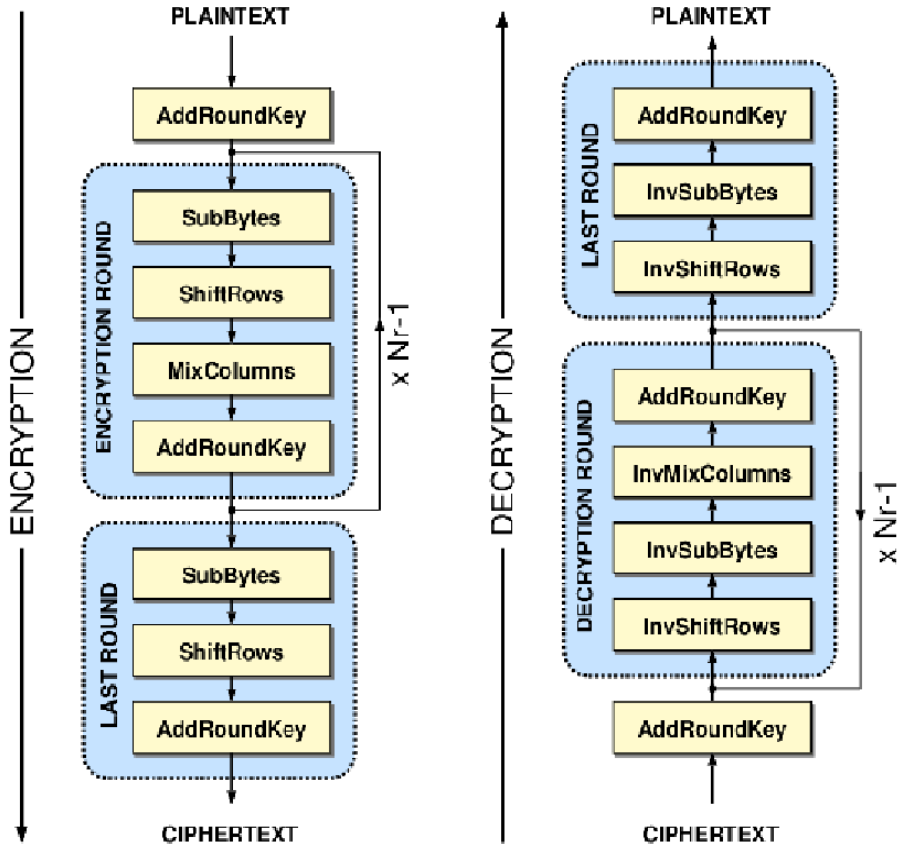
(1) التعويض **SubByte**

(2) التبديل **Rotation**

(3) خلط الاعمدة **MixColumn**

(4) إضافة مفتاح مستدير **AddRounKey**

وبالنسبة لعملية فك التشفير فتكون العملية عكسية.[43]



الشكل 8.4: هيكل AES

4.4 التنفيذ

من اجل الوصول للهدف الأساسي لهذا البحث والذي يتمثل في نمذجة نظام العميل/الخادم وإدخال التشفير عليه من اجل تحقيق أمن المعلومات قد قمنا بالتجربة التي سنشرحها تفصيليا فيما يأتي والتي استعملنا فيها نظام لغة جافا كلغة برمجة.

- **لغة البرمجة المستعملة Java**

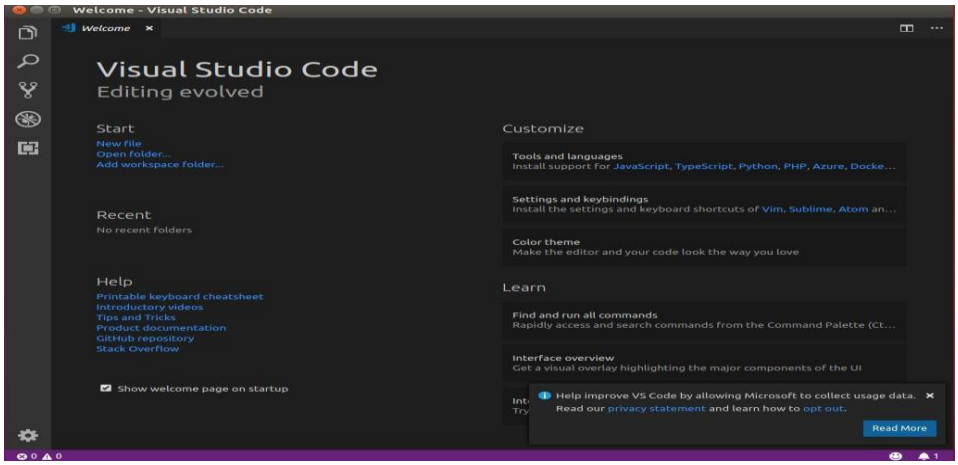
هي لغة برمجة موجهة على نطاق واسع ومنصة برمجية تعمل على مليارات الأجهزة ، بما في ذلك أجهزة الكمبيوتر المحمولة والأجهزة المحمولة ووحدات التحكم في الألعاب والأجهزة الطبية وغيرها الكثير. تستند قواعد وبناء جملة Java على لغات C و C ++. [44]

تدمج Java المفاهيم الأكثر إثارة للاهتمام لتقنيات الكمبيوتر الحديثة في منصة تطوير غنية ومتجانسة ، تم تطوير Java بواسطة SUN in بداية التسعينيات بهدف زيادة قابلية النقل من جهاز إلى آخر ، و موثوقة للغاية ، وبالتالي فهي بيئة برمجة موجهة للكائنات.

تم تصميم Java أيضًا لتكون سهلة الاستخدام وبالتالي فهي سهلة الكتابة والتجميع والتصحيح والتعلم أكثر من لغات البرمجة الأخرى. هذا يسمح لنا بإنشاء برنامج معياري ورمز قابل لإعادة الاستخدام. [24]

visual studio code

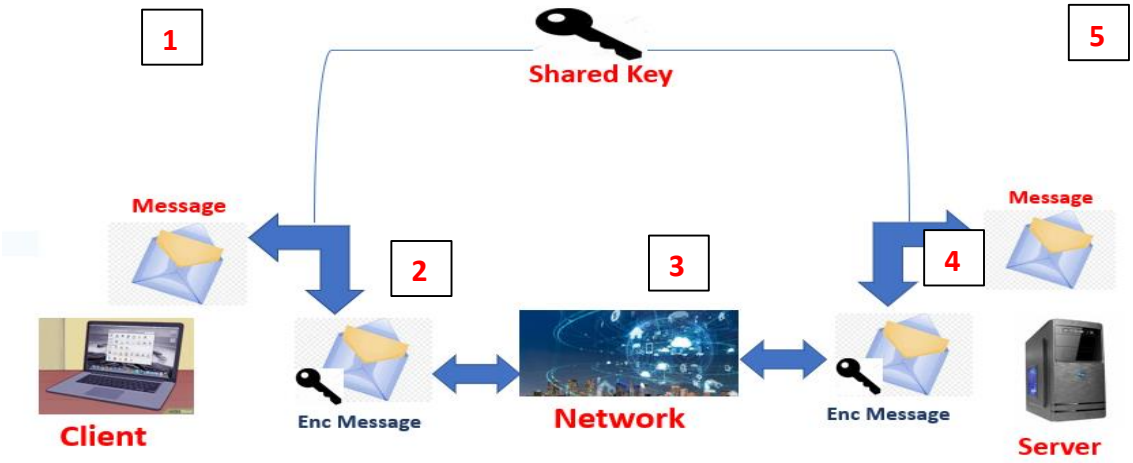
Visual Studio Code ، الذي يشار إليه أيضًا باسم VS Code ، هو محرر شفرة مصدر تم إنشاؤه بواسطة Microsoft لأنظمة Windows و Linux و macOS. تتضمن الميزات دعمًا لتصحيح الأخطاء وإبراز بناء الجملة وإكمال التعليمات البرمجية الذكي والمقتطفات وإعادة بناء التعليمات البرمجية. وهو ما سنقوم بعمل البرمجة عليه في بحثنا.



الشكل 9.4: برنامج visual studio code

- **نموذج الخادم/العميل باستعمال تشفير AES**

بصفة عامة يمكن أن نقوم أن تجربتنا أو موضوعنا عبارة عن تنفيذ أو طريقة إرسال الملفات أو Data من العميل إلى الخادم بطريقة مشفرة حيث أننا وفي هذا العمل قد قمنا باستعمال تشفير AES الذي يعتبر الأنجح والمسموح به عالميا نظرا لموثوقيته وتطوره. وفي هذه المذكرة سنقوم بشرح مفصل لكل جزء من أجزاء هذا النظام.



الشكل 10.4: شكل حول النظام من العميل إلى الخادم

تمت هذه العملية باتباع الخطوات التالية:

1_ العميل يكتب رسالة ليقوم بإرسالها.

2_ يقوم العميل بتشفير هاته الرسالة.

3_ يقوم هذا الأخير بإرسالها عبر الشبكة.

4_ يستلم الخادم هاته الرسالة المشفرة.

5_ يقوم الخادم بفك تشفير محتواها وقراءتها.

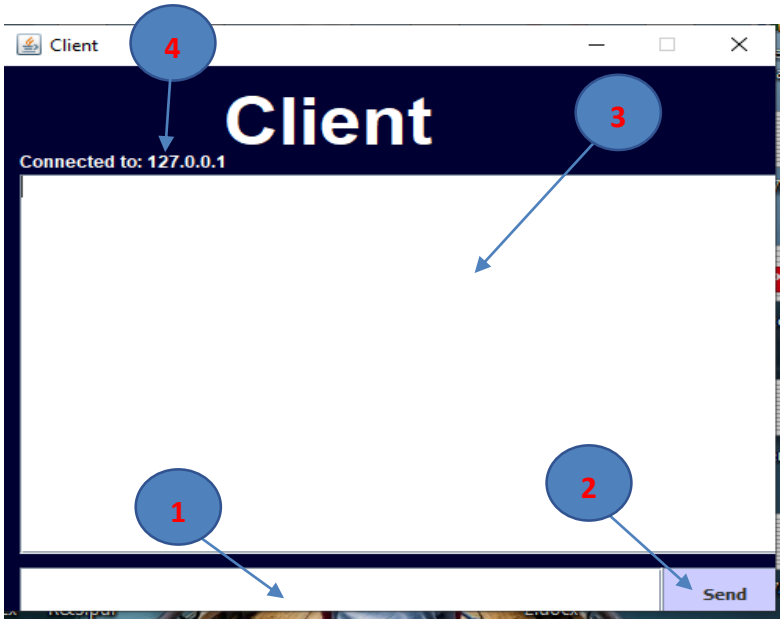
وهذه العملية عكسية فيمكن أن تكون من الخادم باتجاه العميل.

- **جانب العميل**

بالنسبة للنموذج الذي عملنا عليه فهو عبارة عن لغة تحاور بين العميل والخادم أي تبادل الرسائل النصية المكتوبة من العميل الى الخادم والعكس أيضا باستخدام عملية التشفير المتقدم AES .

فهنا بالنسبة للعميل فيقوم بكتابة رسالة ومن ثم ارسالها الى الخادم حث يمكنه أيضا استقبال رسائل الخادم المشفرة والذي يقوم بفك تشفيرها وقراءتها.

الواجهة الرسومية للعميل



الشكل 11.4: الواجهة الرسومية للعميل

1= مكان كتابة الرسالة من طرف العميل.

2= زر ارسال الرسالة.

3= واجهة تكتب فيها الرسالة المرسلة أو الرسالة المشفرة التي استقبلها مع فك التشفير

4= العنوان.

أهم الأوامر

انشاء مقبس وربطه برقم المنفذ والعنوان الخاص بالعميل الذي يمكن التواصل به مع الخادم

```
connection = new Socket(InetAddress.getByName(serverIP),port);
```

استخدام تقنية التشفير AES

```
private static final String ALGORITHM = "AES";
```

انشاء secretkey

```
 secretKey = new SecretKeySpec(key, ALGORITHM);
```

انشاء مساحة لإظهار الحوار المتبادل المشفر والغير مشفر

```
JOptionPane.showMessageDialog(null,"Server Might Be
Down!","Warning",JOptionPane.WARNING_MESSAGE);
```

ارسال رسالة للعميل

```
private void sendMessage(String message)
```

تشفير الرسالة التي قام بإرسالها

```
String encryptedmsg = encyrDecry.encrypt(message, secretKey);
```

تشفير وفك تشفير الرسائل المرسلة والمستقبلة

```
 EncryDecry encyrDecry = new EncryDecry();
```

اظهار الرسالة المستقبلة

```
chatArea.append("\n"+message);
```

اظهار الرسالة التي قام العميل بإرسالها بنفسه

```
 chatArea.append("\nME(Client) - "+message);
```

رقم المنفذ

```
private int port = 1234;
```

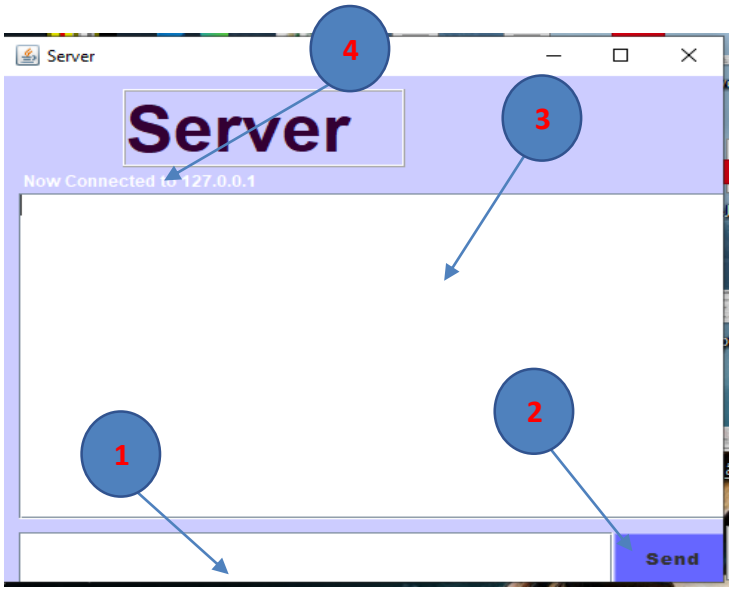
المفتاح المشترك

```
 final static String secretKey = "wissamchahra";
```

- **جانب الخادم**

وفي هذا الجانب أيضا نفس خاصية العمل للعميل بحيث يمكنه أيضا ارسال واستقبال الرسائل مع خاصية التشفير وفك التشفير ل AES

الواجهة الرسومية للخادم



الشكل 12.4: الواجهة الرسومية للخادم

1= مكان كتابة الرسالة من طرف الخادم.

2= زر ارسال الرسالة.

3= واجهة تكتب فيها الرسالة المرسلة أو الرسالة المشفرة التي استقبلها مع فك التشفير.

4= العنوان الذي تتعامل معه حاليا.

أهم الأوامر

انشاء مقبس وربطه برقم المنفذ الذي يمكن للعملاء التواصل به مع الخادم عبره من خلال الأمر

```
server=new ServerSocket(port, totalClients);
```

قبول الرسالة المبعوثة اليه

```
connection=server.accept();
```

اظهار الرسالة المستقبلة

```
chatArea.append("\n"+message);
```

إمكانية التواصل وارسال رسالة للعميل أيضا من خلال

```
sendMessage(jTextField1.getText());
    jTextField1.setText("");
```

اظهار الرسالة التي قام الخادم بإرسالها بنفسه

```
chatArea.append("\nME(Server) - "+message);
```

استخدام تقنية التشفير AES

```
private static final String ALGORITHM = "AES";
```

انشاء secretkey

```
 secretKey = new SecretKeySpec(key, ALGORITHM);
```

تشفير الرسالة التي قام بإرسالها

```
String encryptedmsg = encyrDecry.encrypt(message, secretKey);
```

تشفير وفك تشفير الرسائل المرسلة والمستقبلة

```
 EncryDecry encyrDecry = new EncryDecry();
```

عدد العملاء المسموح لهم بالتواصل والتواصل معهم

```
private int totalClients = 100;
```

رقم المنفذ

```
private int port = 1234;
```

المفتاح المشترك

```
 final static String secretKey = "wissamchahra";
```

البرنامج 2

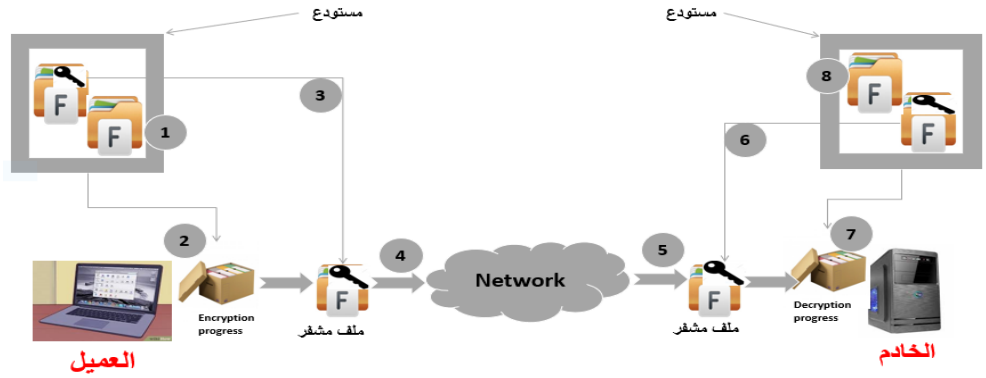
Netbeans

NetBeans عبارة عن بيئة تطوير متكاملة (IDE) لـ Java. يسمح NetBeans بتطوير التطبيقات من مجموعة من مكونات البرامج المعيارية تسمى الوحدات النمطية. يعمل NetBeans على أنظمة تشغيل Windows و macOS و Linux و Solaris. بالإضافة إلى تطوير Java ، فإنه يحتوي على امتدادات للغات أخرى مثل PHP و C و C ++ و HTML5 و JavaScript. يمكن توسيع التطبيقات القائمة على NetBeans ، بما في ذلك NetBeans IDE ، بواسطة مطوري الطرف الثالث.

الشكل13.4: Netbeans

ارسال الملفات والصور باستعمال نموذج العميل/الخادم بالتشفير المتقدم AES

حسب الشرح المبدئي لهذه التجربة يمكن أن نقول أنها عبارة عن ارسال ملفات من العميل الى الخادم بطريقة مشفرة حيث استعملنا تشفير AES كخوارزمية تشفير مضمونة ويعمل بها دوليا حيث يقوم الخادم بدوره هنا وهو فك التشفير. والصورة التالية تعطي فكرة أولية أو نظرة عامة لمبدئ العمل.



الشكل14.4: أهم عمليات تطبيق العميل/الخادم

الأرقام في الصورة تمثل

1= العميل يختار الملف

2= يقوم بتشفير هذا الملف

3= يحتفظ بنسخة مشفرة

4= يرسل الملف المشفر عبر الشبكة

5= الخادم يستلم الملف

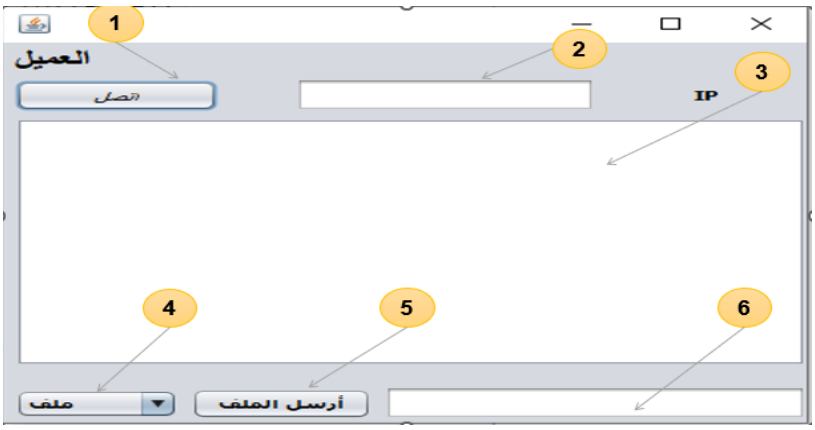
6= يحتفظ بنسخة مشفرة

7= يقوم بفك تشفير الملف

8= يحفظ بالملف غير المشفر

جانب العميل

يعتمد تصميم هذا الجانب ليعمل كعميل ويكمن دوره في ارسال ملفات مشفرة للخادم لضمان سريتها. فبعد تأكيد الاتصال بين كليهما يقوم العميل باختيار ملف أو صورة وتشفيره باستعمال خوارزمية AES ومن ثم يرسلها للخادم الذي يستلمه ويخزنه. والشكل التالي يبرز الواجهة الرسومية للعميل.



الشكل15.4: الواجهة الرسومية للعميل

يمكن للعميل الاتصال بالخادم على نفس الجهاز وهذا ما قمنا به في هاته التجربة وان كان يريد التواصل مع خادم من جهاز اخر فعليه ادخال قيمة العنوان IP.

دليل الأرقام

1= زر للتواصل مع الخادم

2= مكان كتابة عنوان الجهاز المراد التواصل معه

3= منطقة تظهر لنا الحوار المتبادل

4= زر اختيار نوع ما سنرسله صورة أو ملف

5= زر لاختيار الملف وارساله

6= منطقة تظهر اسم الملف المختار

أهم الأوامر

يمكن أن نلخص أهم أوامر هذا الجانب فيما يلي:

- انشاء مقبس وتوصيله برقم المنفذ المتعلق بالعنوان المحدد

```
socket = new Socket((addressField.getText().trim().isEmpty() ?
InetAddress.getLocalHost().getHostAddress(): addressField.getText()), 9999);
```

- أمر من أجل اختيار الملف المراد ارساله

```
JFileChooser filechooser = new JFileChooser(); int c =
filechooser.showOpenDialog(this);
```

- تحويل مفتاح String AES الى SecretKey لاستخدامه في التشفير

```
byte[] decodedKey = Base64.getDecoder().decode(key.trim());

SecretKey secretKey = new SecretKeySpec(decodedKey, 0, decodedKey.length,
"AES");
```

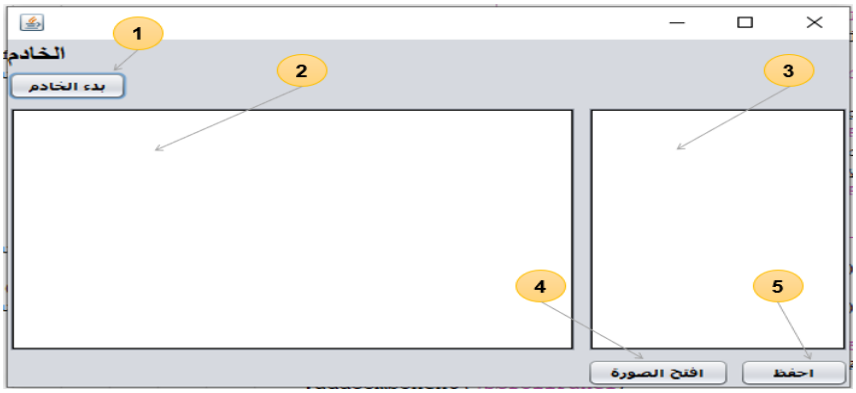
- انشاء كائن مسؤول عن خطوات عملية التشفير لخوارزمية AES

```
Cipher cipher = Cipher.getInstance("AES");

cipher.init(Cipher.ENCRYPT_MODE, secretKey);
```

جانب الخادم

صمم هذا الجانب من أجل استلام أو استقبال الملفات المرسلة من طرف العميل. حث أنه في البداية يقوم بفتح الاتصال وانتظار اتصال العميل به وعند قبوله وقيام العميل بإرسال ملف مشفر يستلم النسخة المشفرة ويفك تفيرها وان أراد الاحتفاظ بها في الجهاز فبإمكانه ذلك أو فتحه اذا كانت صورة. والصورة .... تمثل الواجهة الرسومية للخادم



الشكل16.4: الواجهة الرسومية للخادم

دليل الأرقام

1= زر لبدء تشغيل الخادم.

2= منطقة لإبراز التواصل المتبادل.

3= منطقة اظهار اسم الملف المشفر المرسل.

4= زر فتح الصورة.

5= زر لحفظ ما تم استلامه وك تشفيره.

أهم الأوامر

اما بالنسبة لأوامر جانب الخادم فنلخصها فيما يلي:

- انشاء مقبس وتوصيله برقم المنفذ المحدد لكي يتواصل معه العملاء.

server = new ServerSocket(9999);

- عند قبول الاتصال تظهر رسالة توضح ذلك

```
txt.append("خادم جديد " + name1 + " تم الاتصال معه ...\n");
```

- الخادم في انتظار أي ملف يرسل اليه من طرف المتصل

```
txt.append(name1 + " يمكن ارسال ملف حاليا ...\n");
```

- استلام الملف المشفر وفك تشفيره باستعمال المفتاح المشترك

```
data = (Data) inputStream.readObject();
byte decryptedBytes[] = decryptBytes(data.getFile(), AES_KEY);
```

- فتح الملف إذا كان عبارة عن صورة

```
if (data.getStatus().equals("صورة")) {
                ShowImage obj = new ShowImage(this, true);
                ImageIcon icon = new ImageIcon(data.getFile());
                obj.set(icon);
                obj.setVisible(true);
```

- حفظ الملف بعد فك التشفير

```
Data data = (Data) mod.getElementAt(list.getSelectedIndex());
JFileChooser ch = new JFileChooser();
int c = ch.showSaveDialog(this);
```

5.4 خاتمة

نهاية هذا الفصل عبارة عن تحقيق الهدف المراد والمطلوب ألا وهو التحقق من الاتصال بين العميل والخادم بطريقة مشفرة ومضمونة والتمكن من فك التشفير فقد قمنا بشرح الخطوات التي مررنا بها في هذا العمل والمتمثلة في شرح الهيكل العام لهذا النموذج وطريقة التشفير المختارة ثم شرح العمل الذي قمنا به في تطبيقنا من واجهة رسومية وتشفير مقترح وتحقق الاتصال المباشر عبارة عن تأكيد بأن التجربة قد تمت ومن هنا ننهي الفصل.

الخلاصة العامة

الحواسيب وعلم الشبكات جزء لا يتجزأ من حياتنا اليوم وأهمية المعلومات التي تخزنها وتوصلها إلى المجتمع لا غنى لأي فرد عنها.

منحنا هذا المشروع فرصة التعرف على واحدة من أهم البنى الموزعة وهي بنية الخادم/العميل كما منحنا فرصة التعرف على كيفية تعامل هذا النموذج مع التهديدات التي تتعرض إليها البيانات في الشبكة.

مع زيادة التهديدات وتطور طرق سرقة البيانات تتطور حلول الحماية من هذه المخاطر، مع استمرارية تطور التشفير ظهرت خوارزمية AES كواحدة من أروع الحلول.

في مشروعنا هذا، اعتمدنا معيار التشفير المتقدم AES ذلك أنه أكثر الشفرات استخدما لتشفير البيانات كما انه يعمل بسرعة كبيرة تسمح بتنفيذ العمليات بسرعة وببساطة تنفيذ على الأجهزة والبرامج.

يستخدم تشفير المفتاح المتماثل مفتاح سري واحد لتشفير وفك تشفير المعلومات السرية ويتم استخدام نفس الخوارزمية والمفتاح في كلا الاتجاهين ويجد هذا النوع من التشفير الترحيب في نموذج الخادم/العميل وباستخدامنا خوارزمية AES على النموذج رأينا كيف كانت فعالة للغاية وكيف تم تشفير وفك التشفير البيانات سريعا جدا.

كنتيجة تم الوصول إليها نرى ان التطبيق كان يعمل في الوضع المتصل ويظهر لنا المنفذ وعنوان IP المستخدم في تطبيق الخادم/العميل وتتجلى لنا رؤية النص المشفر وفك تشفيره في وقت قياسي.

المراجع

[1] Team, B. I. (2022, March 08). What Is the Client-Server Model? (Plus Definition and Functions). Récupéré sur **https://www.indeed.com/career-advice/career-development/what-is-client-server-model.**

[2] **Kumar, S**. (2019, August 07). **A REVIEW ON CLIENT-SERVER BASED APPLICATIONS AND RESEARCH OPPORTUNITY** 33858 . I*nternational Journal of Scientific Research*,DOI: http://dx.doi.org/10.24327/ijrsr.2019.1007.3768 **https://www.researchgate.net/publication/335015436**

[3] Client-serveur - Définition et Explications. (s.d.). Récupéré sur

https://www.techno- science.net/definition/3743.html

[4] *Client-Server*. (2022). Récupéré sur **https://www.heavy.ai/technical-glossary/client-server.**

[5] B. Souheyla, **«E Etude et Administration des Systèmes de Supervision dans un Réseau Local »** ,Master's Thesis In Science , University of Abou Bakr Belkaid Tlemcen,Department Of Science,2011 et **https://www.clicours.com/les-differents-modeles-de-client-serveur/**

[6]Oliver, G. e. (2000). ***Le Client-Serveur***. BYROLLES Bld Saint-Germain,61Paris Cedex 0575240.

[7] H. Yazid H. Soumia, **« Conception et réalisation d'une application client-serveur en utilisant le Middleware JAVA RMI (gestion des absences) »** ,Master's thesis in informatique, University of Abou Bakr Belkaid Tlemcen Department Of Informatique, 2017

[8] D.E.COMER , **" Computer Networks and Internets**",Upper Saddle River,New Jersey 07458,2009.

[9] Singh, S. C. (2009)." ***An Introduction to CLIENT/SERVE COMPUTIN"***. Daryaganj, New DelhiNew Age International (p)Ltd.Publishers,Ansari Road. Récupéré sur www.newagepublishers.com

[10] INGALLS, S. (2021, November 17). *What Is a Client-Server Model? A Guide to Client-Server Architecture*. Récupéré sur https://www.serverwatch.com/guides/client-server-model/.

[11] A. Hayat. B. Meriem, **« Conception et réalisation d'une application Client/Serveur pour la gestion de parc Informatique Cas : Fonds National d'Investissement »**,Master's thesis in Informatique,University of Mouloud MAMMERI ,Tizi-Ouzou Department Of Informatique,2012

[12] https://www.javatpoint.com/computer-network-client-and-server-model

[13] احمد حسن مشايخ, CCNA ROUTING AND SWITCHING.

[14]LEMODELETCP/IP,https://www.lyceerotroudreux.com/images/NSI/modele_tcpip.pdf

[15] Renaud Lachaize," **Communication par sockets TCP/IP Illustration avec Java",** Université Grenoble Alpes ,Janvier 2020, https://du-isn.gricad-pages.univ-grenoble-alpes.fr/2-sr/Reseaux/3--cours_reseaux--sockets_java.pdf

[16]Professor: Panagiota Fatourou **"Introduction to Sockets Programming in C using TCP/IP"** TA: Eleftherios Kosmas CSD - May 2012

[17] 2 -ème année LMD **"Les Sockets"** Université Mohamed Khider – Biskra Année Universitaire 2015/2016

[18] Alexandre.Sedoglavic@univ-lille1.fr **"Prise de communication (socket)"** Licence miage — Université Lille 1 Semestre 6 — 2012-2013

[19] M. Belguidoum **"Programmation réseau en java : les sockets"** Université Mentouri de Constantine Département Informatique

[20] **"Communications inter-processus Les Sockets" PDF**

[21]IBM I 7.1 https://www.ibm.com/docs/en/i/7.1?topic=programming-how-sockets-work Copyright IBM Corporation 2012

[22] IBM z/OS 2.4.0 https://www.ibm.com/docs/en/zos/2.4.0?topic=internets-socket-api Copyright IBM Corporation 2015, 2021

[23] tutorialspoint https://www.tutorialspoint.com/what-is-interprocess-communication#:~:text=Interprocess%20communication%20is%20the%20mechanism,from%20one%20process%20to%20another.

[24] Sayah Tarek **"Conception of client/Server System with Encrypted Data Exchanging Using Sockets"** 25 june 2018

[25] https://www.edureka.co/blog/socket-programming-in-java/#:~:text=Socket%20programming%20in%20Java%20is,a%20client%20and%20a%20server

[26]http://etutorials.org/Programming/Pocket+pc+network+programming/Chapter+1.+Winsock/Connectionless+UDP+Sockets/ eTutorials.org

[27]Priya Pedamkar https://www.educba.com/types-of-socket/

[28]Daniel LAMAS, La cryptographie, Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES, Haute École de Gestion de Genève (HEG-GE) Filière Informatique de Gestion, 5 juin 2015

[29] Saiful Azad Al-Sakib Khan Pathan " PRACTICAL CRYPTOGRAPHY Algorithms and Implementations Using C++ "Apple Academic Press Inc Oakville ,Canada ,31 Oct 2015, http://www.crcpress.com/product/isbn/9781482228892

[30] http://dspace.univ-tlemcen.dz/bitstream/112/6836/1/Etude-comparative-entre-la-cryptographie.pdf

[31]كبما, م. (2015, 26يونيو). *قلب أمن المعلومات ..مقدمة عن التشفير*. Récupéré sur arageek.com/tech/encryptin-the-core-of-data-security.

[32] M , Bokhari Qahtan .M, Shallal. (2016, August). A Review on Symmetric Key Encryption Techniques in Cryptography. *nternational Journal of Computer Applications*. nternational Journal of Computer Applications, August 2016, : https://www.researchgate.net/publication/333118027

[33] https://www.technawi.net/ مدخل إلى - علم التشفير – أنواع - التشفير 18 سبتمبر،2016

[34] Ait Ameur Yacine Mehdi, Sécurisation des communications dans les réseaux d'ordinateurs (couche SSL) »,Master's thesis in electronique,University ofMohamed Khider,Biskra Department Of Informatique,2014

[35]https://arabicprogrammer.com/article/7306567335/

[36]Stinson, D. (s.d.). *Cryptographie Théorie et pratique.* O CRC Press,Inc,2002,Paris ,www.vuibert.fr

[37]https://fr.wikipedia.org/wiki/Data_Encryption_Standard

[38]J.-Y.Chouinard,"Design of Secure Computer Systems",Notes on the Data Encryption Standard(DES),University of Laval,Québec,Canada,September 23,200é.

[39]JoanDaemenVincentRijmen"The_Design_of_Rijndael_The_Advanced_Encryption_Standard_AES_Second_Edition"

[40]Houda FERRADI **"Introduction à la cryptographie (cours 4): Chiffrement par bloc (AES)"** Université Paris 13 Villetaneuse 01/02/2016

[41]Jean-Marc Robert **"Cryptologie Algorithmes à clé secrete"** Génie logiciel et des TI

[42] Pierre-Alain Fouque **"Algorithmes de chiffrement symétrique par bloc (DES et AES)"** Equipe de Cryptographie Ecole normale supérieure

[43] Avi Kak (kak@purdue.edu**) "Lecture 8: AES: The Advanced Encryption Standard Lecture Notes on "Computer and Network Security""** ©2022 Avinash Kak, Purdue University February 3, 2